The average number of amicable pairs and aliquot cycles for a family of elliptic curves

James Parks

A Thesis
in
The Department
of
Mathematics and Statistics

Presented in Partial Fulfillment of the Requirements
for the Degree of Doctor of Philosophy (Mathematics) at
Concordia University
Montréal, Québec, Canada

August 2013

CONCORDIA UNIVERSITY
SCHOOL OF GRADUATE STUDIES

This is to certify that the thesis prepared

By: **James Parks**

Entitled: **The average number of amicable pairs and aliquot cycles for a family of elliptic curves**

and submitted in partial fulfillment of the requirements for the degree of

DOCTOR OF PHILOSOPHY (Mathematics)

complies with the regulations of the University and meets the accepted standards with respect to originality and quality.

Signed by the final examining committee:

Approved by _____ Chair
Approved by Dr. A. Jain

Approved by_____ External Examiner
Approved by Dr. D. Koukoulopoulos

Approved by_____ External to Program
Approved byDr. P. Bianucci

Approved by_____ Examiner
Approved byDr. A. Iovita

Approved by_____ Examiner
Approved byDr. C. Cummins

Approved by_____ Thesis Supervisor
Approved byDr. C. David

Approved by _____
Approved by Chair of Department or Graduate Program Director
Dr. J. Garrido, Graduate Program Director

August 27, 2013 _____

Dr. N. Esmail
Professor J. Locke, Interim Dean
Faculty of Arts and Science

ABSTRACT

The average number of amicable pairs and aliquot cycles for a family of elliptic curves

James Parks, Ph.D.

Concordia University, 2013

Let E be an elliptic curve over $\mathbb{Q}$. Silverman and Stange defined the set $(p_1, \ldots, p_L)$ of distinct primes to be an *aliquot cycle* of length L of E if each p_i is a prime of good reduction for E such that

$$\#E_{p_1}(\mathbb{F}_{p_1}) = p_2, \ldots, \#E_{p_{L-1}}(\mathbb{F}_{p_{L-1}}) = p_L, \#E_{p_L}(\mathbb{F}_{p_L}) = p_1.$$

Let $\pi_{E,L}(X)$ denote the aliquot cycle counting function with $p \leq X$. They conjectured for elliptic curves without complex multiplication that $\pi_{E,L}(X) \asymp \sqrt{X}/(\log X)^L$. Jones refined this conjecture to give an explicit constant, namely

$$\pi_{E,L} \sim C_{E,L} \frac{\sqrt{X}}{(\log X)^L}.$$

In this thesis we will show that the conjectured upper bound holds for $\pi_{E,L}(X)$ on average over the family of all elliptic curves with a short length for the average.

Acknowledgements

First, I would like to thank my supervisor, Dr. Chantal David, for all her helpful and insightful feedback in the theory of analytic number theory and elliptic curves and for her patience and guidance in the writing of this thesis.

Secondly, I would like to thank Dr. Hershy Kisilevsky and Dr. Dimitris Koukoulopoulos for their courses on L-functions and sieve methods, which have been of great interest to me and benefit in the work on this thesis.

I would also like to thank the remaining thesis committee members and Marie-France Leclere for all of her help.

I would like to thank Daniel Fiorilli and Anders Södergren for all their great advice and insight into our work on the MRC project and all the fun and productive meetings we've had.

I would like to thank all my fellow classmates, especially Jungbae Nam and Patrick Meisner, for all their help as well as the rest of the students in the number theory group in Montreal and graduate students at Concordia for helping to make my time in Montreal so rewarding.

Lastly, I would like to thank the People's Potato for all the delicious vegan food and amazing friends and for making life as a graduate student at Concordia a truly unique and remarkable experience.

Contents

Chapter 1

Introduction

Let E be an elliptic curve over $\mathbb{Q}$. Then E can be expressed by the equation

$$E : y^2 = x^3 + ax + b, \quad a, b \in \mathbb{Q}$$

with discriminant $\Delta_E = -16(4a^3+27b^2) \neq 0$. For each prime $p \nmid \Delta_E$, E reduces to a curve over $\mathbb{F}_p$ with $\#E(\mathbb{F}_p) = p + 1 - a_p(E)$, where $E_p(\mathbb{F}_p)$ is the group of points on E over $\mathbb{F}_p$ and $|a_p(E)| \leq 2\sqrt{p}$ by the Hasse bound. There are several conjectures associated with the reductions E_p as p varies over the primes $p \leq X$, such as the Sato-Tate conjecture for the distribution of the normalized traces $\left\{ \dfrac{a_p(E)}{2\sqrt{p}} \right\}$ for $p \leq X$, or the Lang-Trotter conjecture [LaTr] for the number of primes $p \leq X$ such that $a_p(E) = t$ for a fixed integer t, or the Koblitz conjecture [Kob] for the number of primes $p \leq X$ such that $\#E(\mathbb{F}_p) = p+1-a_p(E)$ is prime. The Sato-Tate conjecture was recently proven for elliptic curves over totally real fields which have multiplicative reduction at some prime by Harris, Shepherd-Barron and Taylor [HSBT], but the other conjectures are completely open. For example, we do not know if there exist infinitely many primes $p \leq X$ such that $a_p(E) = t$ for any elliptic curve over $\mathbb{Q}$, except when $t = 0$, which corresponds to the supersingular case. This was considered by Elkies [Elk] who showed that every elliptic curve E over $\mathbb{Q}$ has infinitely many supersingular primes. We discuss the above conjectures in greater detail in Chapter

3.

In a recent paper, Silverman and Stange [SiSt2] suggested a new question related to the distribution of the reductions of a global elliptic curve. For a positive integer $L \geq 2$, Silverman and Stange define an L-tuple $(p_1, \ldots, p_L)$ of distinct prime numbers to be an *aliquot cycle* of length L of E if E has good reduction at each prime p_i, where E_{p_i} denotes the reduced curve, such that for $1 \leq i \leq L-1$,

$$\#E_{p_i}(\mathbb{F}_{p_i}) = p_i + 1 - a_p(E_{p_i}) = p_{i+1} \text{ and } \#E_{p_L}(\mathbb{F}_{p_L}) = p_1.$$

Aliquot cycles of length $L = 2$ are defined to be *amicable pairs*.

Remark 1.0.1. The definitions of aliquot cycles and amicable pairs arise as the elliptic curve analogues to the classically defined aliquot cycles and amicable numbers. For an integer $n \geq 2$ we define

$$\sigma(n) := \sum_{d|n} d,$$

to be the sum of divisors function and we define $s(n) := \sigma(n) - n$ to be the sum of proper divisors function. Classically, aliquot cycles, also called *sociable numbers*, are a set of integers $(m_1, \ldots, m_n)$ satisfying

$$s(m_1) = m_2, \ldots, s(m_{n-1}) = m_n, s(m_n) = m_1.$$

Aliquot cycles of length two are called *amicable numbers*, for example, $(220, 284)$. Aliquot cycles of length one, the case when $s(n) = n$, are called *perfect numbers*.

For an elliptic curve $E/\mathbb{Q}$ we say that an aliquot cycle $(p_1, \ldots, p_L)$ is *normalized* if $p_1 = \min\{p_i : 1 \leq i \leq L\}$ and we define the aliquot cycle counting function as

$$\begin{aligned}\pi_{E,L}(X) :=& \#\{p_1 \leq X | (p_1, \ldots, p_L) \text{ is a normalized aliquot cycle}\} \\ =& \#\{(p_1, \ldots, p_L) \text{ is a normalized aliquot cycle} \mid p_1 \leq X\}.\end{aligned}$$

Throughout this thesis we will use the following standard notation.

Definition 1.0.2. We say that $f(x) = O(g(x))$ if and only if there exists a positive real number C and a real number x_0 such that

$$|f(x)| \leq C|g(x)| \text{ for all } x > x_0,$$

and we say that $f \ll_n g$ if and only if $f \in O_n(g)$, where the subscript n is used to denote that the implicit constant is a function of n. We also say that $f(x) \asymp g(x)$ if and only if there exist positive constants C_1, C_2 and a real number x_0 such that

$$C_1|g(x)| \leq |f(x)| \leq C_2|g(x)| \text{ for all } x > x_0,$$

and we say that $f(x) \sim g(x)$ if and only if

$$\lim_{x\to\infty} \frac{f(x)}{g(x)} = 1.$$

The goal of this thesis is to study the behavior of the aliquot cycle counting function. As in the case of other distributions questions, it is easy to predict the number of amicable pairs and aliquot cycles with the following simple heuristic. Let $L = 2$ and let E be an elliptic curve without complex multiplication, then we have that

$$\pi_{E,L}(X) \approx \sum_{p\leq X} \text{Prob}(p + 1 - a_p(E) := q \text{ is prime and } q + 1 - a_q(E) = p).$$

If these events are independent then we have that

$$\begin{aligned}\pi_{E,L}(X) &\approx \sum_{p\leq X} \text{Prob}(p+1-a_p(E) := q \text{ is prime}) \cdot \text{Prob}(q+1-a_q(E)=p) \\ &\approx \sum_{p\leq X} \frac{1}{\log p} \cdot \frac{1}{4\sqrt{p}} \\ &\approx \frac{\sqrt{X}}{\log^2 X},\end{aligned}$$

by the prime number theorem and the Hasse bound. Silverman and Stange [SiSt2] generalized this argument to give the following conjecture.

Conjecture 1.0.3. *Let $E/\mathbb{Q}$ be an elliptic curve and let $L \geq 2$. Assume that there are infinitely many primes p_i such that $\#E_{p_i}(\mathbb{F}_{p_i})$ is prime. Then as $X \to \infty$ we have*

$$\begin{aligned}\pi_{E,L}(X) &\asymp \frac{\sqrt{X}}{(\log X)^L} \quad \text{if } E \text{ does not have complex multiplication,} \\ &\sim A_E \frac{X}{(\log X)^2} \quad \text{if } E \text{ has complex multiplication and } L=2,\end{aligned}$$

where the implied constants in $\asymp$ are both positive and depend only on E and L and A_E is a precise positive constant, although no formula for A_E is given.

Using further heuristic arguments, Conjecture 1.0.3 was refined by Jones [Jon2] to give an explicit constant, $C_{E,L}$. We will explain the heuristic argument of Jones in more detail in Chapter 3.

Remark 1.0.4. We may interpret the case $L = 1$ in Conjecture 1.0.3 as describing primes p for which $\#E_p(\mathbb{F}_p) = p$. These primes are called *anomalous primes* and have been considered previously by Mazur [Maz]. Anomalous primes are to be avoided in cryptography because the elliptic curve discrete logarithm problem for anomalous primes can be solved in linear time, [SiSt2] and in this case, Conjecture 1.0.3 is a special case of a conjecture of Lang and Trotter [LaTr], with $t = 1$, see Conjecture 3.1.20.

To gain further evidence for the distribution conjectures mentioned above, it is natural

to consider the average for these conjectures over some family of elliptic curves. Thus, to gain insight into the number of amicable primes and aliquot cycles, we will consider the average of $\pi_{E,L}(X)$ for a family of elliptic curves. Throughout this thesis, we define our family of elliptic curves as

$$\mathcal{C} := \mathcal{C}(A, B) = \{E_{a,b} : Y^2 = X^3 + aX + b, a, b \in \mathbb{Z}, |a| \leq A, |b| \leq B\}$$

which is a two parameter family of elliptic curves with nonzero discriminant. Since the number of elliptic curves that have complex multiplication is small with respect to the size of the family of all elliptic curves, we hope to find on average over all curves that as $X \to \infty$,

$$\frac{1}{|\mathcal{C}|} \sum_{E \in \mathcal{C}} \pi_{E,L}(X) \sim C_L \frac{\sqrt{X}}{(\log X)^L},$$

where C_L is related to conjectural constants given by Jones [Jon2], which we discuss in Chapter 3.

Note that in the $L = 2$ case we have that for an amicable pair (p, q), given a prime p, the Hasse bound implies that $q \in (p + 1 - 2\sqrt{p}, p + 1 + 2\sqrt{p})$, and hence we will be required to count the number of primes in this short interval, where not even the Riemann Hypothesis guarantees the existence of a prime. Thus, we will need to assume some conjectures about the distribution of primes in short intervals to get an average result for $\pi_{E,L}(X)$. This is similar to another distribution question related to elliptic curves that was considered by David and Smith [DaSm1], where the authors showed that under a suitable hypothesis for the number of primes of size X in an interval of length $X^{\frac{1}{2}-\epsilon}$ for some $\epsilon > 0$, the number of primes p such that $\#E(\mathbb{F}_p) = p + 1 - a_p(E) = N$ for a fixed integer N has the expected asymptotic, on average over all elliptic curves in the family described above. In that case, we also have that $\#E(\mathbb{F}_p) = p + 1 - a_p(E) = N$ implies that $p \in (N + 1 - 2\sqrt{N}, N + 1 + 2\sqrt{N})$.

We now state the two main goals of this thesis.

The first goal is to obtain the conjectured upper bound for the average number of

aliquot cycles for a family of elliptic curves. That is, we will show unconditionally for $L \geq 2$ that

$$\frac{1}{|\mathcal{C}|} \sum_{E \in \mathcal{C}} \pi_{E,L}(X) \ll_L \frac{\sqrt{X}}{(\log X)^L},$$

with some bounds on A and B by using the fundamental lemma of the combinatorial sieve, as given by Friedlander and Iwaniec [FrIw1]. These calculations are primarily performed in Section 3.2 and Chapter 4.

The length of the average is of course an important feature of average results, and there are several techniques that were developed to obtain short (and possibly optimal) averages for the distribution questions associated with the reduction of a global curve. For the Sato-Tate conjecture (when the size of the intervals varies with p, which is not covered by the results of Harris, Shepherd-Barron and Taylor), and the Koblitz conjecture, it was shown by Banks and Shparlinski [BanShp] and Balog-Cojocaru-David [BCD] respectively, that the asymptotic over the family $\mathcal{C}(A, B)$ can be obtained as long as $A, B > X^{\epsilon}$ and $AB > X^{1+\epsilon}$ for some $\epsilon > 0$. The same technique was applied by Baier [Ba2] to the Lang-Trotter conjecture, but in that case, it leads to an average of size $A, B > X^{\epsilon}$ and $AB > X^{3/2+\epsilon}$. This is caused by the fact that the set of elliptic curves over $\mathbb{F}_p$ with a fixed trace $a_p(E)$ is far thinner (among all elliptic curves over $\mathbb{F}_p$) than the set of elliptic curves over $\mathbb{F}_p$ for which the group of points has prime order. We remark that for both the case of the Lang-Trotter and Koblitz conjecture, the "trivial length of the average" would be $A, B > X^{1+\epsilon}$.

The second goal of the thesis is to generalize the techniques used by Banks and Shparlinski [BanShp] and Balog, Cojocaru and David [BCD] to the context of aliquot cycles. This leads to an average length $A, B > X^{\epsilon}$ and $AB > X^{\frac{3L}{2}+\epsilon}$, for some $\epsilon > 0$. We remark that for the problem of aliquot cycles of length L the "trivial length of the average" is $A, B > X^{L+\epsilon}$, as shown in Section 3.2. The short length of the average is obtained in Chapter 5. As in [BCD], we use multiplicative characters to detect the isomorphism class of the reduction of the elliptic curve $E(a, b)$ modulo p, and then bounds on character

sums and the large sieve to get a short average. Because we have L-tuples of primes $(p_1, \dots, p_L)$ for the case of aliquot cycles, we need to consider products of characters modulo the primes p_i, and the question of primitivity becomes more critical, as explained in Chapter 5.

The first and second goal can be summarized in the following result.

Theorem 1.0.5. *Let $\epsilon > 0$, $E/\mathbb{Q}$ be an elliptic curve and let $\mathcal{C}$ be the family of elliptic curves with*

$$A, B > X^{\epsilon}, \qquad X^{\frac{3L}{2}}(\log X)^6 < AB < e^{X^{\frac{1}{6}-\epsilon}}.$$

Then as $X \to \infty$ we have that

$$\frac{1}{|\mathcal{C}|}\sum_{E\in\mathcal{C}} \pi_{E,L}(X) \ll \frac{\sqrt{X}}{(\log X)^L},$$

where the implied constant depends on L only.

Note that the additional condition $AB < e^{X^{\frac{1}{6}-\epsilon}}$ is not a limiting constraint since we are mainly interested in averages for small values of A and B.

Average results can give strong evidence for the distribution conjectures, because they also verify the conjectural constants which are obtained from heuristic arguments based on local probabilities and the distribution of Frobenius elements in the field extensions given by the ℓ-torsion of elliptic curves. See Chapter 3.1 for more details of this process for the case of several distribution conjectures, and for an explicit description of the constant $C_{E,L}$ obtained by Jones with this heuristic.

Chapter 2

Background

2.1 Elliptic curves

In this section we will give a basic introduction into the theory of elliptic curves. Many of the necessary definitions and results are standard and given in Silverman [Sil1, Chapter III].

Before we give the definition of an elliptic curve we recall the following two definitions from algebraic geometry.

Definition 2.1.1. The *genus* of a connected, orientable surface is an integer representing the maximum number of cuttings along non-intersecting closed simple curves without rendering the resultant manifold disconnected. It is equal to the number of handles on it.

Remark 2.1.2. *The sphere and disc both have genus zero and a torus has genus one.*

Definition 2.1.3. Let K be a field. We define *projective n-space*, $\mathbb{P}^n$ as the set of all $(n+1)$-tuples

$$\{P = (x_0, \ldots, x_n) : x_i \in \overline{K}, \text{ for } 0 \leq i \leq n\}$$

such that at least one x_i is nonzero modulo the equivalence relation given by

$$(x_0, \ldots, x_n) \sim (y_0, \ldots, y_n)$$

if there exists a $\lambda \in \overline{K}^*$ with $x_i = \lambda y_i$ for $0 \leq i \leq n$.

The formal definition of an elliptic curve is as follows.

Definition 2.1.4. Let K be a field. An *elliptic curve* E is defined to be a non-singular, projective algebraic curve of genus one along with the *point at infinity*, $\mathcal{O} := [0 : 1 : 0]$ in $\mathbb{P}^2$. If E is defined over K then E can be given by the *Weierstrass equation*,

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \text{ with } a_1, \ldots, a_6 \in K.$$

If $\text{char}(\overline{K}) \neq 2$ then replacing y by $\frac{1}{2}(y - a_1x - a_3)$ gives an equation of the form

$$E : y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6,$$

where

$$b_2 = a_1^2 + 4a_2, \quad b_4 = 2a_4 + a_1a_3 \quad \text{and} \quad b_6 = a_3^2 + 4a_6.$$

We also define the quantities

$$\begin{aligned} b_8 &:= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2, \\ c_4 &:= b_2^2 - 24b_4, \\ c_6 &:= -b_2^3 + 36b_2b_4 - 216b_4, \\ \Delta &:= -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6, \\ j &:= \frac{c_4^3}{\Delta}. \end{aligned}$$

Definition 2.1.5. The quantity Δ given above is called the *discriminant* of the Weierstrass equation and j is called the *j-invariant* of an elliptic curve.

Furthermore, if $\text{char}(\overline{K}) \neq 2, 3$ then replacing (x, y) by $\left(\frac{x - 32b_2}{36}, \frac{y}{108}\right)$ gives the simpler equation

$$E : y^2 = x^3 - 27c_4x - 54c_6.$$

Remark 2.1.6. In this paper we are primarily interested in elliptic curves over the fields $K = \mathbb{Q}$ or $\mathbb{F}_p$ where p is a prime greater than three. In these cases we can write a *short Weierstrass equation* for our elliptic curve given by

$$E_{A,B} : y^2 = x^3 + Ax + B, \text{ with } A, B \in K. \tag{2.1}$$

In this case we have that

$$\Delta = -16(4A^3 + 27B^2), \quad j = \frac{-1728(4A)^3}{\Delta}.$$

In the definition of an elliptic curve above we required that the curve be non-singular. We give the following criteria for a curve given by the Weierstrass equation to be singular. This is given in Silverman [Sil1, Proposition 3.1.4].

Proposition 2.1.7. *(a) The curve given by a Weierstrass equation can be classified as follows.*
(i) It is non-singular if and only if $\Delta \neq 0$.
(ii) It has a node if and only if $\Delta = 0$ *and* $c_4 \neq 0$.
(iii) It has a cusp if and only if $\Delta = c_4 = 0$.
In cases (ii) and (iii) there is only one singular point.
(b)Two elliptic curves are isomorphic over $\overline{K}$ *if and only if they have the same* j*-invariant.*

Throughout this thesis we are mainly interested in considering elliptic curves defined over $\mathbb{Q}$ given by the short Weierstrass equation

$$E : y^2 = x^3 + Ax + B, \text{ with } A, B \in \mathbb{Z},$$

and then considering the same equation defined over finite fields $\mathbb{F}_p$ where p is a prime greater than three and determining if the reduced equation also describes an elliptic curve over $\mathbb{F}_p$. This is equivalent to checking if $\Delta \not\equiv 0 \pmod{p}$.

Definition 2.1.8. Let $E/\mathbb{Q}$ be an elliptic curve. We say that E has *good reduction* at a prime p if $\Delta \not\equiv 0 \pmod{p}$ and denote the reduced curve by E_p, and we say that E has *bad reduction* otherwise.

Since we are interested in Weierstrass equations of elliptic curves that when reduced modulo various primes have as good reduction as often as possible we give the following definition.

Definition 2.1.9. Let E be an elliptic curve given by a Weierstrass equation. We say that the Weierstrass equation is *minimal* at a prime p if the largest power of p dividing Δ cannot be reduced by an admissible change of variables. Furthermore, we say that the Weierstrass equation is a *global minimal Weierstrass equation* if it is minimal at every p.

Additionally, we have the further classification of reduction of an elliptic curve given in Silverman [Sil1, VII.5].

Definition 2.1.10. Let E/K be an elliptic curve and let E_p be the reduced curve for a minimal Weierstrass equation.
(a) E has *good* (or *stable*) *reduction* over K if E_p is non-singular.
(b) E has *multiplicative* (or *semi-stable*) *reduction* over K if E_p has a node.
(c) E has *additive* (or *unstable*) *reduction* over K if E_p has a cusp.
In cases (b) and (c) we say that E has *bad reduction*. If E has multiplicative reduction, then the reduction is said to be *split* (respectively *non-split*) if the slopes of the tangent lines at the node are in K (respectively not in K).

Remark 2.1.11. Let E be an elliptic curve given by a global minimal Weierstrass equation. Then we can associate an invariant called the *conductor*, N_E of E related to the discriminant Δ. The set of primes dividing Δ coincides exactly with the set of primes dividing the conductor. Except for the primes 2 and 3, the power of the prime p diving N_E is either 1 or 2, depending whether E has a node or a cusp $\pmod{p}$ respectively. The power of the primes 2 and 3 dividing the conductor can be determined by Tate's algorithm described in Silverman [Sil2, Chapter IV.9].

Remark 2.1.12. The points on an elliptic curve form an abelian group under the composition law for adding points on an elliptic curve. If E is defined over K then we let $E(K)$ denote the group of points on E and we have that

$$E(K) = \{(x, y) \in K^2 : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6\} \cup \{\mathcal{O}\}$$

is a subgroup of E. The criterion for the composition law is given in Silverman [Sil1, Proposition III.2.2].

We also have the following celebrated theorem of Mordell for the group of points on the elliptic curve, $E(K)$, in the special case $K = \mathbb{Q}$ given in Silverman [Sil1, Theorem VIII.4.1].

Theorem 2.1.13. ***(Mordell-Weil Theorem for*** $K = \mathbb{Q}$***)*** *Let $E/\mathbb{Q}$ be an elliptic curve then the group $E(\mathbb{Q})$ is a finitely generated abelian group. That is,*

$$E(\mathbb{Q}) \cong \mathbb{Z}^r \times E_{\text{tors}}(\mathbb{Q}),$$

where the torsion subgroup $E_{\text{tors}}(\mathbb{Q})$ is finite and the algebraic rank r of $E(\mathbb{Q})$ is a non-negative integer.

We now provide definitions and results about maps between elliptic curves.

Definition 2.1.14. Let E_1, E_2 be elliptic curves. We define a *morphism* $\phi : E_1 \to E_2$ to be a rational map which is regular at every point. If $\phi(\mathcal{O}) = \mathcal{O}$ then ϕ is called an *isogeny*. We say that E_1 and E_2 are *isogenous* if there is an isogeny ϕ between them with $\phi(E_1) \neq \{\mathcal{O}\}$.

Definition 2.1.15. Let

$$\text{Hom}(E_1, E_2) := \{\text{isogenies } \phi : E_1 \to E_2\}.$$

If $E_1 = E_2$ then we define $\text{End}(E)$:=$\text{Hom}(E, E)$ to be the *endomorphism ring*.

We have the following classification of endomorphism rings given in Silverman [Sil1, Corollary III.9.4].

Proposition 2.1.16. *Let E/K be an elliptic curve. Then End(E) is either $\mathbb{Z}$, an order in a quadratic imaginary field or an order in a quaternion algebra. Moreover, if char(K) = 0, only the first two cases occur.*

Definition 2.1.17. Let E be an elliptic curve over a field K with $\mathrm{char}(K) = 0$. We say that E has *complex multiplication* if the endomorphism ring $\mathrm{End}(E) \supsetneq \mathbb{Z}$.

From the formulation of an elliptic curve in (2.1) we can determine the necessary and sufficient conditions for two elliptic curves to be isomorphic.

Definition 2.1.18. Let $E = E_{a,b}$ and $E' = E_{a',b'}$ be elliptic curves defined over a field K with discriminants Δ and Δ' respectively. An *isomorphism* $E \to E'$ is defined to be an element u in K^* for which $a' = u^4 a, b' = u^6 b$ and $\Delta' = u^{12}\Delta$. An *automorphism* of E is defined to be an isomorphism $E \to E$ and we use the symbol $\overline{E}$ to denote a representative from an isomorphism class of E.

Definition 2.1.19. Let E be an elliptic curve defined over $\mathbb{F}_p$ for some prime p. We define the *Frobenius automorphism* to be the map

$$\begin{aligned} \phi_p : & E \to E \\ & (x, y) \mapsto (x^p, y^p), \\ & \mathcal{O} \mapsto \mathcal{O}, \end{aligned}$$

and the characteristic polynomial of ϕ_p is given by

$$f_E(T) = T^2 - a_p(E)T + p$$

where $a_p(E)$ is defined to be the *trace of the Frobenius*.

The trace of the Frobenius provides a way to precisely determine the size of the group of points on an elliptic curve over $\mathbb{F}_p$. For an elliptic curve E with conductor N_E, if $p \nmid N_E$ then

$$a_p(E) = p + 1 - \#E(\mathbb{F}_p).$$

The definition of $a_p(E)$ is extended to the set of all primes by setting

$$a_p(E) := \begin{cases} 1 & \text{if } E \text{ has split multiplicative reduction at } p, \\ -1 & \text{if } E \text{ has non-split multiplicative reduction at } p, \\ 0 & \text{if } E \text{ has additive reduction at } p. \end{cases}$$

We now state the general form of Hasse's Theorem given in Silverman [Sil1, Theorem 5.1.1], although throughout this thesis we will be primarily concerned with the case when q is prime.

Theorem 2.1.20. ***(Hasse's Theorem)*** *Let E/K be an elliptic defined over the field with q elements. Then*

$$|\#E(K) - q - 1| \leq 2\sqrt{q}.$$

The following theorem gives a classification of the possible automorphism groups of E described in detail in Silverman [Sil1, Theorem III.10.1].

Theorem 2.1.21. *Let E/K be an elliptic curve. Then its automorphism group* Aut(E) *is a finite group of order given by*

$$\#\text{Aut(E)} = \begin{cases} 2 & \text{if } j(E) \neq 0, 1728, \\ 4 & \text{if } j(E) = 1728 \text{ and } \mathrm{char}(K) \neq 2, 3, \\ 6 & \text{if } j(E) = 0 \text{ and } \mathrm{char}(K) \neq 2, 3, \\ 12 & \text{if } j(E) = 0 = 1728 \text{ and } \mathrm{char}(K) = 3, \\ 24 & \text{if } j(E) = 0 = 1728 \text{ and } \mathrm{char}(K) = 2. \end{cases}$$

For elliptic curves over $\mathbb{F}_p$ this can be stated more succinctly as follows.

Corollary 2.1.22. *Let $E/\mathbb{F}_p$ be an elliptic curve with $p > 3$ given by*

$$E : y^2 = x^3 + ax + b.$$

Then its automorphism group Aut(E) *is given by*

$$\#\mathrm{Aut(E)} = \begin{cases} 6 & \text{if } a = 0 \text{ and } p \equiv 1 \pmod 3, \\ 4 & \text{if } b = 0 \text{ and } p \equiv 1 \pmod 4, \\ 2 & \text{otherwise.} \end{cases}$$

We now consider the number of elliptic curves over $\mathbb{F}_p$. This is given in Lenstra [Len].

Proposition 2.1.23. *Let $E/\mathbb{F}_p$ be an elliptic curve with p a prime greater than three given by*

$$E : y^2 = x^3 + ax + b$$

and let $\overline{E}$ denote a representative of an isomorphism class of E. Then

$$\sum_{E \in \mathbb{F}_p} 1 = (p-1) \sum_{\overline{E} \in \mathbb{F}_p} \frac{1}{\#\mathrm{Aut}(\overline{\mathrm{E}})} = p^2 - p.$$

With the goal of proving a result of Deuring [Deu], we consider the following definitions.

Definition 2.1.24. Let D be a negative integer. We define a *positive definite integral binary quadratic form* to be a homogeneous polynomial of the form $Q(X, Y) = aX^2 + bXY + cY^2$ with $a, b, c \in \mathbb{Z}, a > 0$ satisfying $D = b^2 - 4ac < 0$, where D is defined to be the *discriminant of* $Q(X, Y)$. A discriminant D is called a *fundamental discriminant* if $D = 1$ or D is the discriminant of a quadratic field.

We have the following conditions for fundamental discriminants. Specifically, D is a fundamental discriminant if and only if either $D \equiv 1 \pmod 4$ and is square-free or

$D = 4m$ where $m \equiv 2, 3 \pmod 4$ and m is square-free. The following definition relates discriminants to the class numbers of the ring of integers of imaginary quadratic fields.

Definition 2.1.25. Let N be a non-negative integer, the *Hurwitz-Kronecker class number*, $H(N)$, is defined when $N = 0$ or $N \equiv 1, 2 \pmod 4$ as

$$H(N) := \begin{cases} \frac{-1}{12} & \text{if } N = 0, \\ 0 & \text{if } N \equiv 1, 2 \pmod 4. \end{cases}$$

Otherwise, $H(N)$ is the number of classes of not necessarily primitive, positive definite quadratic forms of discriminant $-N$; except that the classes which have a representative that is a multiple of the form $x^2 + y^2$ should be counted with weight $\frac{1}{2}$ and the classes which have a representative that is a multiple of the form $x^2 + xy + y^2$ should be counted with weight $\frac{1}{3}$.

We can relate the Hurwitz-Kronecker class number to the usual class number as follows, Lenstra [Len].

Remark 2.1.26. Given a (not necessarily fundamental) discriminant $D < 0$, the Hurwitz-Kronecker class number of discriminant D is defined by

$$H(D) = \sum_{\substack{f^2 | D \\ \frac{D}{f^2} \equiv 0,1 \pmod 4}} \frac{h\left(\frac{D}{f^2}\right)}{w\left(\frac{D}{f^2}\right)}, \tag{2.2}$$

where $h(d)$ denotes the usual class number of the unique imaginary quadratic order of discriminant $d < 0$ and $w(d)$ denotes the size of its unit group.

We now state the important result of Deuring [Deu] which will be of great use in the following chapters.

Theorem 2.1.27. ***(Deuring's Theorem)*** *Let $E/\mathbb{Q}$ be an elliptic curve, let $\overline{E}$ denote a representative of an isomorphism class of E, let $p > 3$ be a prime and let t be an integer*

such that $t^2 - 4p < 0$. *Then*

$$\sum_{\substack{\overline{E}\in\mathbb{F}_p \\ a_p(\overline{E})=t}} \frac{1}{\#\mathrm{Aut}(\overline{E})} = H(t^2-4p),$$

where the sum is over the $\mathbb{F}_p$ *isomorphism classes of elliptic curves.*

2.2 Dirichlet characters and analytic number theory

In this section we will provide the basic definitions of arithmetic functions and Dirichlet characters. We also include important results in analytic number theory and sieve methods that will be necessary in the following chapters. In this section and throughout the thesis, for integers m and n, we let (m,n) denote the greatest common divisor of m and n and we let $[m,n]$ denote the least common multiple of m and n.

Definition 2.2.1. An *arithmetic function* is a real or complex valued function $f(n)$ defined on the set of natural numbers. We say that $f(n)$ is *additive* if $f(mn) = f(m)+f(n)$ if $(m,n) = 1$ and *completely additive* when $f(mn) = f(m) + f(n)$ for all $m, n \in \mathbb{N}$. We say that $f(n)$ is *multiplicative* if $f(mn) = f(m)f(n)$ when $(m,n) = 1$ and *completely multiplicative* if $f(mn) = f(m)f(n)$ for all $m, n \in \mathbb{N}$.

Example 2.2.2. Let p be a prime, then we define $\nu_p(n)$ to be the highest power of the prime p that divides n. That is, if $p \mid n$ then $n = p^{\nu_p(n)}k$ where $(p,k) = 1$. We have that $\nu_p(n)$ is an additive arithmetic function.

Example 2.2.3. We define $\varphi(n)$, the Euler totient function to be the number of positive integers not greater than n that are coprime to n. We have that

$$\varphi(n) = n\prod_{p\mid n}\left(1-\frac{1}{p}\right),$$

and $\varphi(n)$ is a multiplicative function, where for a non-negative integer k we have that

$$\varphi(p^k) = \begin{cases} p^{k-1}(p-1) & \text{if } k \geq 1, \\ 1 & \text{if } k = 0. \end{cases}$$

We have the following useful properties of the Euler φ-function.

Proposition 2.2.4. *Let m, n be integers then we have that*

1. $\varphi(mn) = \varphi(m)\varphi(n)\frac{(m,n)}{\varphi((m,n))}$.
2. $\varphi([m,n]) = \frac{\varphi(m)\varphi(n)}{\varphi((m,n))}$.

We also have the following bounds for arithmetic functions that we make use of in the following chapters. The first is a bound for the Euler φ-function given in [BacSha, Theorem 8.8.7].

Theorem 2.2.5. *We have that*

$$\varphi(x) \leq x \ll \varphi(x) \log\log x.$$

We also have the more general result on bounds for multiplicative functions, given in [Te, Theorem 1.11].

Theorem 2.2.6. *Let f be a multiplicative function. If there exist constants A, B such that*

$$\sum_{p \leq x} f(p) \log p \leq Ax \quad (x \geq 1), \quad \text{and} \quad \sum_{\substack{p \text{ prime} \\ v \geq 2}} \frac{f(p^v)\log(p^v)}{p^v} \leq B,$$

then for $x \geq 2$ we have that

$$\sum_{n \leq x} f(n) \leq (A + B + 1)e^B \frac{x}{\log x} \prod_{p \leq x} \left(1 + \frac{f(p)}{p}\right).$$

We have that two arithmetic functions can be related in the following way.

Definition 2.2.7. Let f, g be arithmetic functions. We define the *Dirichlet convolution* of f and g, by

$$(f * g)(n) := \sum_{d|n} f(d) g\left(\frac{n}{d}\right).$$

We also require the following definition for arithmetic functions.

Definition 2.2.8. Let f be an arithmetic function, then we denote the *formal Dirichlet series* attached to f as

$$L(s, f) := \sum_{n=1}^{\infty} \frac{f(n)}{n^s}.$$

If f is a multiplicative function then

$$L(s, f) = \prod_{p} \left(\sum_{v=0}^{\infty} \frac{f(p^v)}{p^{vs}} \right).$$

Example 2.2.9. If $f(n) = 1$ then $\zeta(s) := L(s, 1)$ is the Riemann zeta function which is absolutely convergent for $\mathrm{Re}(s) > 1$.

Remark 2.2.10. The definition of multiplicative functions can be extended to multivariate functions as well. We say that $f(n_1, \ldots, n_k)$ is multiplicative if $n_i = n_i' n_i''$ for $1 \leq i \leq k$ with $(n_1' \cdots n_k', n_1'' \cdots n_k'') = 1$ then $f(n_1, \ldots, n_k) = f(n_1', \ldots, n_k') f(n_1'', \ldots, n_k'')$. Combining this with the definition of a formal Dirichlet series gives

$$\sum_{n_1=1}^{\infty} \cdots \sum_{n_k=1}^{\infty} f(n_1, \ldots, n_k) = \prod_{p} \left(\sum_{v_1=0}^{\infty} \cdots \sum_{v_k=0}^{\infty} f(p^{v_1}, \ldots, p^{v_k}) \right).$$

For the remainder of this section we focus on the theory of Dirichlet characters, which are completely multiplicative functions. Many of the necessary definitions and results are given in Davenport [Dav, Chapter 4,5].

Definition 2.2.11. A *Dirichlet character* of modulus q is defined to be any function

$$\chi : \mathbb{Z} \to \mathbb{C},$$

which has the following properties.

1. There exists a positive integer q such that $\chi(n) = \chi(n+q)$ for all n.
2. If $(n,q) > 1$ then $\chi(n) = 0$, if $(n,q) = 1$ then $\chi(n) \neq 0$, is a root of unity.
3. $\chi(mn) = \chi(m)\chi(n)$ for all $m, n \in \mathbb{Z}$.

That is, χ is a completely multiplicative function that is periodic with period q.

Definition 2.2.12. Fix an integer $q \in \mathbb{N}$. The character

$$\chi_0(n) := \begin{cases} 1 & \text{if } (n,q) = 1, \\ 0 & \text{otherwise,} \end{cases}$$

is called the *trivial* or *principal character* to the modulus q.

Definition 2.2.13. Let $\chi(n)$ be any character to the modulus q other than the principal character. If $(n,q) = 1$ and $\chi(n)$ has period less than q then we say that χ is *imprimitive* and otherwise *primitive*.

The following propositions are given in Davenport [Dav, Chapter 4, 5].

Proposition 2.2.14. *Let χ be an imprimitive character to the modulus q. Then there exists a proper factor q_1 of q and a primitive character $\chi_1 \pmod{q_1}$ such that*

$$\chi(n) := \begin{cases} \chi_1(n) & \text{if } (n,q) = 1, \\ 0 & \text{if } (n,q) > 1. \end{cases}$$

Remark 2.2.15. We say that χ has *conductor* q_1 if χ is imprimitive and if χ is primitive then χ has conductor $q = q_1$. We also have for any Dirichlet character $\pmod{q}$ that there are $\varphi(q)$ characters.

We also have the following orthogonality relations for Dirichlet characters.

Proposition 2.2.16. *Let χ be a Dirichlet character to the modulus q. Then we have that*

$$\sum_{n=1}^{q} \chi(n) = \begin{cases} \varphi(q) & \text{if } \chi = \chi_0, \\ 0 & \text{otherwise,} \end{cases}$$

$$\sum_{\chi \pmod q} \chi(n) = \begin{cases} \varphi(q) & \text{if } n \equiv 1 \pmod q, \\ 0 & \text{otherwise,} \end{cases}$$

where the summation in the second sum is over all the $\varphi(q)$ characters.

We can use the previous result to construct a linear combination of the characters which selects those integers n which fall in a given reduced residue class $\pmod q$.

Theorem 2.2.17. *Let χ be a Dirichlet character to the modulus q and let $\overline{\chi}$ denote its complex conjugate. If $(a, q) = 1$ then*

$$\frac{1}{\varphi(q)} \sum_{\chi \pmod q} \overline{\chi}(a)\chi(n) = \begin{cases} 1 & \text{if } n \equiv a \pmod q, \\ 0 & \text{otherwise.} \end{cases}$$

We now focus on the specific case of real Dirichlet characters. We begin by giving the following definitions of the Legendre and Kronecker symbol.

Definition 2.2.18. Let a, n be integers. If there exists an integer x such that $x^2 \equiv a \pmod n$ then a is called a *quadratic residue* $\pmod n$ and otherwise, a *quadratic non-residue* $\pmod n$. If p is an odd prime then the *Legendre symbol* is an arithmetic function of a and p that is defined as follows:

$$\left(\frac{a}{p}\right) := \begin{cases} 1 & \text{if } a \text{ is a quadratic residue } \pmod p \text{ and } a \not\equiv 0 \pmod p, \\ -1 & \text{if } a \text{ is a quadratic non} - \text{residue } \pmod p, \\ 0 & \text{if } a \equiv 0 \pmod p. \end{cases}$$

Remark 2.2.19. The Legendre symbol has the following two important properties.

1. The Legendre symbol $\left(\frac{\cdot}{p}\right)$ is a completely multiplicative Dirichlet character (mod q).
2. Let p and q be odd primes. The *law of quadratic reciprocity* can be stated as

$$\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)(-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

Definition 2.2.20. Let $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ be a positive integer where $(p_1, \ldots, p_k)$ are odd primes. Let a be any integer then the *Jacobi symbol* is defined as

$$\left(\frac{a}{n}\right) := \left(\frac{a}{p_1}\right)^{\alpha_1} \cdots \left(\frac{a}{p_k}\right)^{\alpha_k},$$

where $\left(\frac{a}{p_i}\right)$ is the Legendre symbol. The *Kronecker symbol*, $\left(\frac{a}{n}\right)$ is the extension of the Jacobi symbol to all integers by the following definitions.

$$\left(\frac{a}{2}\right) := \begin{cases} 0 & \text{if } a \equiv 0 \pmod 2, \\ 1 & \text{if } a \equiv \pm 1 \pmod 8, \\ -1 & \text{if } a \equiv \pm 3 \pmod 8, \end{cases}$$

$$\left(\frac{a}{-1}\right) := \begin{cases} -1 & \text{if } a < 0, \\ 1 & \text{if } a \geq 0, \end{cases}$$

$$\left(\frac{a}{0}\right) := \begin{cases} 1 & \text{if } a = \pm 1, \\ 0 & \text{otherwise.} \end{cases}$$

We have the following classification of real primitive characters given in Davenport [Dav, Chapter 5].

Theorem 2.2.21. *Let $\left(\frac{d}{n}\right)$ be the Kronecker symbol. Then the real primitive characters $\chi(n)$ are precisely the $\chi(n) = \left(\frac{d}{n}\right)$ where d is a fundamental discriminant and d can be*

expressed as a product of relatively prime factors of the form

$$-4,\ 8,\ -8,\ (-1)^{\frac{p-1}{2}}p\ \ (p>2),$$

and $\chi(n)$ is a real primitive character to the modulus $|d|$.

The real non-principal characters are also called quadratic characters. We now state the large sieve inequality for Dirichlet characters which is discussed in Davenport [Dav, Chapter 27].

Theorem 2.2.22. *(**The large sieve inequality**) Let M, N, Q be positive integers and let $\{a_n\}_n$ be a sequence of complex numbers. For a fixed $q \leq Q$, we let χ be a Dirichlet character modulo q. Then*

$$\sum_{q\leq Q}\frac{q}{\phi(q)}\sum_{\substack{\chi \pmod q\\ \chi \text{ primitive}}}\left|\sum_{M<n\leq M+N}a_n\chi(n)\right|^2 \leq (N+3Q^2)\sum_{M<n\leq M+N}|a_n|^2.$$

We now define an L-function for a Dirichlet character.

Definition 2.2.23. Let $\chi(n)$ be a Dirichlet character to the modulus q. We define the *Dirichlet L-function* associated to χ

$$L(s,\chi) := \sum_{n=1}^{\infty}\frac{\chi(n)}{n^s} = \prod_p\left(1-\frac{\chi(p)}{p^s}\right)^{-1} \quad \text{for } \mathrm{Re}(s)>1.$$

Remark 2.2.24. *By analytic continuation this function can be continued to a meromorphic function on the complex plane. Dirichlet showed that $L(s,\chi)\neq 0$ for $s=1+it$ and if $\chi=\chi_0$ then*

$$L(s,\chi_0) = \zeta(s)\prod_{p|q}(1-p^{-s}),$$

which has a simple pole at $s=1$.

Using the notion of the Hurwitz-Kronecker class number discussed in the previous

section we have the following relationship between a quadratic Dirichlet L-function and the class number, which is discussed in Davenport [Dav, Chapter 6] .

Theorem 2.2.25. ***(Analytic class number formula)*** *Let $D = df^2$ where d is a negative fundamental discriminant and let $\chi_D = \left(\frac{D}{n}\right)$ be the Kronecker symbol. Then χ_D is a Dirichlet character and we have that*

$$\frac{h(d)}{w(d)} = \frac{\sqrt{-D}}{2\pi} L(1, \chi_D), \text{ where } L(s, \chi_D) = \sum_{n=1}^{\infty} \frac{\chi_D(n)}{n^s} \text{ for } s \in \mathbb{C}, \mathrm{Re}(s) > 0,$$

and $w(d)$ is the number of roots of unity in $\mathbb{Q}(\sqrt{d})$.

We wish to bound the $L(1, \chi_D)$ by a short Euler product but first we will give the very useful result of Merten.

Theorem 2.2.26. ***(Mertens' Theorem)*** *Let $z \geq 2$ and let γ denote the Euler-Mascheroni constant then*

$$\prod_{p \leq z} \left(1 - \frac{1}{p}\right) = \frac{e^{-\gamma}}{\log z} \left(1 + O\left(\frac{1}{\log z}\right)\right),$$

where

$$\gamma := \lim_{n \to \infty} \left(\sum_{k=1}^{n} \frac{1}{k} - \log n\right).$$

Let $s \in \mathbb{C}$ with $\mathrm{Re}(s) > 1, y \geq 1$ and χ a Dirichlet character, we define the following notation

$$L(s, \chi; y) := \prod_{p \leq y} \left(1 - \frac{\chi(p)}{p}\right)^{-1}.$$

Then we have the following result given by Granville and Soundararajan [GrSo] essentially due to Elliot.

Lemma 2.2.27. *(Granville, Soundararajan, [GrSo]) Let $\alpha \geq 1$ and $Q \geq 3$. There is a set $\mathcal{E}_\alpha(Q) \subset [1, Q]$ of at most $Q^{\frac{2}{\alpha}}$ integers such that if χ is a Dirichlet quadratic character*

modulo some $q \leq Q$ of conductor not in $\mathcal{E}_\alpha(Q)$, then

$$L(1,\chi) = \prod_{p \leq (\log Q)^{8\alpha^2}} \left(1 - \frac{\chi(p)}{p}\right)^{-1} \left(1 + O_\alpha\left(\frac{1}{(\log Q)^\alpha}\right)\right).$$

This result will be used to bound the error terms in our calculations in Chapter 4. Now, let $P^+(n)$ denote the largest prime dividing n and let $P^-(n)$ denote the smallest prime dividing n. We now state a result which is known as the fundamental lemma of sieve methods which will allow us to give an upper bound for a sum over primes in terms of a sum over integers. This will be a key tool to give the correct upper bound for the average number of aliquot cycles. The version we will use is a direct consequence of [FrIw1, Lemma 5].

Lemma 2.2.28. *(**Fundamental Lemma**)*
Let $y \geq 2, D = y^u$ with $u \geq 2$. There exists two arithmetic functions $\lambda^\pm : \mathbb{N} \to [-1,1]$, supported in the set $\{d \in \mathbb{N} : P^+(d) \leq y, d \leq D\}$, for which

$$\begin{cases} (\lambda^- * 1)(n) = (\lambda^+ * 1)(n) = 1 \text{ if } P^-(n) > y, \\ (\lambda^- * 1)(n) \leq 0 \leq (\lambda^+ * 1)(n) \text{ otherwise.} \end{cases}$$

Moreover, if $g : \mathbb{N} \to \mathbb{R}$ is a multiplicative function with $0 \leq g(p) \leq \min\{2, p-1\}$ for all primes $p \leq y$ then

$$\sum_d \frac{\lambda^\pm(d) g(d)}{d} = \prod_{p \leq y} \left(1 - \frac{g(p)}{p}\right)(1 + O(e^{-u})).$$

Finally, we conclude this section by stating the following useful bound for Dirichlet L-functions given by Friedlander and Iwaniec [FrIw2], which we will make use of in our calculation of the short length of the average in Chapter 5.

Theorem 2.2.29. *(**The fourth power moment of Dirichlet characters**) Let q, N be positive integers. Let χ denote a Dirichlet character modulo q, with χ_0 denoting the*

principal character. Then

$$\sum_{\chi \neq \chi_0} \left| \sum_{n \leq N} \chi(n) \right|^4 \ll N^2 q \log^6 q.$$

Chapter 3

Amicable pairs and aliquot cycles

3.1 Background

In this chapter we give an introduction to the theory of amicable pairs and aliquot cycles for elliptic curves. We first review the previous results of Silverman and Stange [SiSt2] and Jones [Jon2] and in the following section we give an outline of the steps required to obtain an average for the number of aliquot cycles for a family of elliptic curves.

We begin this section by recalling the definition of aliquot cycles and amicable pairs for an elliptic curve over $\mathbb{Q}$.

Definition 3.1.1. Let $E/\mathbb{Q}$ be an elliptic curve. We define an L-tuple $(p_1, \ldots, p_L)$ of distinct prime numbers to be an *aliquot cycle* of length L of E if E has good reduction at each prime p_i, and for $1 \leq i \leq L-1$, we have that

$$\#E_{p_i}(\mathbb{F}_{p_i}) = p_i + 1 - a_{p_i}(E_{p_i}) = p_{i+1} \text{ and } \#E_{p_L}(\mathbb{F}_{p_L}) = p_1.$$

Aliquot cycles of length $L = 2$ are defined to be *amicable pairs*. We say that an aliquot cycle $(p_1, \ldots, p_L)$ is *normalized* if $p_1 = \min\{p_i : 1 \leq i \leq L\}$ and we define the aliquot

cycle counting function as

$$\pi_{E,L}(X) := \#\{p_1 \leq X \mid (p_1, \ldots, p_L) \text{ is a normalized aliquot cycle}\}.$$

Silverman and Stange [SiSt1] were motivated to study aliquot cycles and amicable pairs for elliptic curves upon discovering that these invariants occurred in a natural fashion when they were generalizing to elliptic divisibility sequences Smyth's [Smy] results on index divisibility of Lucas sequences.

From the conjecture on the number of aliquot cycles of Silverman and Stange in Conjecture 1.0.3, we expect that for an elliptic curve E defined over $\mathbb{Q}$ that $\pi_{E,L}(X)$ will exhibit different behavior depending on whether or not E has complex multiplication. This is demonstrated in the following two examples.

Example 3.1.2. Consider the following two elliptic curves without complex multiplication given by

$$E_1 : y^2 + y = x^3 - x \quad \text{and} \quad E_2 : y^2 + y = x^3 + x^2.$$

We have that $\pi_{E_1,2}(10^7) = 1$ where that amicable pair is $(1622311, 1622471)$, and $\pi_{E_2,2}(10^7) = 4$, the smallest of which is $(853, 883)$.

Example 3.1.3. Consider the elliptic curve with complex multiplication given by

$$E_3 : y^2 = x^3 + 2.$$

In this case we have that $\pi_{E_3,2}(10^6) > 800$ where the first four amicable pairs are

$$(13, 19), (139, 163), (541, 571), (613, 661).$$

There are also examples of elliptic curves having aliquot cycles of length $L \geq 3$.

Example 3.1.4. The elliptic curve $y^2 = x^3 - 25x - 8$ has the aliquot triple $(89, 79, 73)$

and the elliptic curve

$$E : y^2 = x^3 + 176209333661915432764478x$$
$$+ 60625229794681596832262$$

has an aliquot cycle

$$(23, 31, 41, 47, 59, 67, 73, 79, 71, 61, 53, 43, 37, 29)$$

of length 14.

In fact, Silverman and Stange [SiSt2, Theorem 5.1] proved the following result.

Theorem 3.1.5. *(Silverman, Stange) For every $L \geq 1$ there exists an elliptic curve $E/\mathbb{Q}$ that has an aliquot cycle of length L. More generally, for any positive integers $L_1, \ldots, L_r$, there exists an elliptic curve $E/\mathbb{Q}$ that has distinct aliquot cycles of lengths $L_1, \ldots, L_r$.*

Their proof of this result is similar to the proof of [Kow, Proposition 4.9], in which Kowalski constructs elliptic curves such that $\#E_p(\mathbb{F}_p)$ is constant for all p in a given Hasse interval.

Remark 3.1.6. It is also possible to produce elliptic curves having no nontrivial aliquot cycles. If $E(\mathbb{Q})_{\text{tors}} \neq \{\mathcal{O}\}$, then $\#E_p(\mathbb{F}_p)$ will be composite for all but finitely many p, since $E(\mathbb{Q})_{\text{tors}} \hookrightarrow E_p(\mathbb{F}_p)$ for all $p \nmid 2\Delta_{E/\mathbb{Q}}$. For example, the elliptic curves $y^2 = x^3 + x$ and $y^2 = x^3 + 1$ do not have any aliquot cycles.

Silverman and Stange [SiSt2, Corollary 6.2, Proposition 8.1] gave the following results in the complex multiplication case.

Theorem 3.1.7. *(Silverman, Stange) Let $E/\mathbb{Q}$ be an elliptic curve with complex multiplication and j-invariant, j_E.*

1. If $j_E \neq 0$ then there are no aliquot cycles of length $L \geq 3$ consisting of primes $p \geq 5$.

2. If $j_E = 0$ then E has no normalized aliquot triple (p, q, r) with $p > 7$.

Remark 3.1.8. From Theorem 3.1.7 we see that elliptic curves with complex multiplication such that $j_E = 0$, cannot have aliquot cycles of length $L = 3$. However, it is unknown if elliptic curves with complex multiplication such that $j_E = 0$ have any aliquot cycles of length greater than three.

Theorem 3.1.7 is a corollary of the more specific result of Silverman and Stange [SiSt2, Theorem 6.1].

Theorem 3.1.9. *(Silverman and Stange, [SiSt2, Theorem 6.1]) Let $E/\mathbb{Q}$ be an elliptic curve and assume that:*

(1) E has complex multiplication by an order $\mathcal{O}_K$ in an imaginary quadratic field $K = \mathbb{Q}(\sqrt{-D})$.

(2) p and q are primes of good reduction for E with $p \geq 5$ and $q = \#E_p(\mathbb{F}_p)$.

(3) $j_E \neq 0$, or equivalently $\mathcal{O}_K \neq \mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$.

Then $D \equiv 3 \pmod 4$, and either

$$\#E_q(\mathbb{F}_q) = p \quad \text{or} \quad \#E_q(\mathbb{F}_q) = 2q + 2 - p.$$

In the conjecture of Silverman and Stange [SiSt2], Conjecture 1.0.3 on the number of aliquot cylces for a given elliptic curve we make the assumption that there are infinitely many primes p such that $\#E_p(\mathbb{F}_p)$ is prime. Therefore, if an elliptic curve $E/\mathbb{Q}$ is to have any aliquot cycles, then it is clearly necessary that there exist primes p such that $E_p(\mathbb{F}_p)$ is prime. This is considered in the Koblitz Conjecture, given in [Kob] and modified by Zywina [Zyw], see Conjecture 3.1.22.

Then Silverman and Stange use Theorem 3.1.9 to give a heuristic justification for the following conjecture [SiSt2, Conjecture 6.9].

Conjecture 3.1.10. *(Silverman and Stange, [SiSt2]) Let $E/\mathbb{Q}$ be an elliptic curve with*

complex multiplication, define

$$\pi_E^{\text{twin}}(X) := \{p \leq X | \#E_p(\mathbb{F}_p) \text{ is prime}\}$$

and assume that $j_E \neq 0$. *Then either* $\pi_E^{\text{twin}}(X)$ *is bounded, or else*

$$\lim_{X\to\infty} \frac{\pi_{E,2}(X)}{\pi_E^{\text{twin}}(X)} = \frac{1}{4}.$$

Remark 3.1.11. From [SiSt2, Remark 6.10], we have that if $E/\mathbb{Q}$ has complex multiplication, then

$$\pi_E^{\text{twin}}(X) \ll \frac{X}{\log^2 X},$$

which yields the same upper bound for $\pi_{E,2}(X)$. Hence, we have an upper bound of the right order of magnitude in Conjecture 1.0.3 for the number of amicable pairs in the complex multiplication case.

We will now discuss the work of Jones [Jon2]. He refined Conjecture 1.0.3 in the non-complex multiplication case as follows, [Jon2, Conjecture 1.3].

Conjecture 3.1.12. *Let* $E/\mathbb{Q}$ *be an elliptic curve without complex multiplication and fix an integer* $L \geq 2$. *Then there is a non-negative real constant* $C_{E,L} \geq 0$ *such that as* $X \to \infty$ *we have that*

$$\pi_{E,L}(X) \sim C_{E,L} \int_2^X \frac{1}{2\sqrt{t}(\log t)^L} dt.$$

Remark 3.1.13. It is possible for the constant $C_{E,L}$ to be zero, in which case as $X \to \infty$ we have that $\pi_{E,L}(X)$ is finite. In particular, let $E/\mathbb{Q}$ be the elliptic curve given by $E : y^2 = x^3 - 3x + 4$. Then Jones [Jon2] has shown that $\pi_{E,2}(10^{12}) = 0$ and assuming the Koblitz Conjecture then $C_{E,2} = 0$.

Remark 3.1.14. By integration by parts, we have that

$$\int_2^X \frac{1}{2\sqrt{t}(\log t)^L} dt = \frac{\sqrt{X}}{\log^L X} + O\left(\frac{\sqrt{X}}{(\log x)^{L+1}}\right).$$

Thus, Conjecture 3.1.12 is consistent with Conjecture 1.0.3.

The conjectural constant $C_{E,L}$ of Jones [Jon2] is obtained from a probabilistic model which adjusts the local probabilities at each prime ℓ, similar to the twin prime constant appearing in the twin prime conjecture given below.

Conjecture 3.1.15. ***(Twin Prime Conjecture)***

$$\#\{p \leq x \mid p+2 \text{ is prime}\} \sim \mathfrak{S}\frac{x}{\log^2 x},$$

where

$$\mathfrak{S} = 2\prod_{\ell \neq 2}\frac{\ell(\ell-2)}{(\ell-1)^2}.$$

There is a simple heuristic used to derive the constant $\mathfrak{S}$ given as follows. For a random integer n, and prime $\ell > 2$, we have that

$$\text{Prob}(\ell \nmid n(n+2)) = \frac{\ell-2}{\ell},$$

whereas

$$\text{Prob}(\ell \nmid n)\text{Prob}(\ell \nmid (n+2)) = \left(\frac{\ell-1}{\ell}\right)^2.$$

Hence,

$$\begin{aligned}\mathfrak{S} =& \frac{\text{Prob}(2 \nmid n(n+2))}{\text{Prob}(2 \nmid n)\text{Prob}(2 \nmid (n+2))}\prod_{\ell \neq 2}\frac{\text{Prob}(\ell \nmid n(n+2))}{\text{Prob}(\ell \nmid n)\text{Prob}(\ell \nmid (n+2))} \\ =& 2\prod_{\ell \neq 2}\frac{\ell(\ell-2)}{(\ell-1)^2} \approx 1.32.\end{aligned}$$

In order to obtain the constant for the distribution conjectures associated with elliptic curves, we need a model for the following local probabilities. We need to determine $\text{Prob}(\ell \nmid p+1-a_p(E))$ in the Koblitz Conjecture, $\text{Prob}((a_p(E) \equiv t \pmod{\ell})$ in the Lang-Trotter Conjecture, and $\text{Prob}\Big(p+1-a_p(E) \equiv q \pmod{\ell} \text{ and } q+1-a_q(E) \equiv p \pmod{\ell}\Big)$ in the Amicable Pairs Conjecture.

We consider the n-th division field $\mathbb{Q}(E[n])$, of E, obtained by adjoining to $\mathbb{Q}$ the x and y-coordinates of the n-torsion $E[n]$ of a given Weierstrass model of E. Since

$$E[n] \simeq \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z},$$

we have that

$$\mathrm{Gal}(\mathbb{Q}(E[n])/\mathbb{Q}) \subseteq \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}).$$

By the following theorem of Serre [Se1], we know that for all but a finite number of primes ℓ (depending on the elliptic curve E), the Galois groups $\mathrm{Gal}(\mathbb{Q}(E[\ell])/\mathbb{Q})$ are as big as possible.

Theorem 3.1.16. *(Serre, [Se1]) Let $E/\mathbb{Q}$ be an elliptic curve without complex multiplication. Then, for all but a finite number of primes ℓ, we have that*

$$\mathrm{Gal}(\mathbb{Q}(E[\ell])/\mathbb{Q}) \simeq \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z}).$$

In order to give probabilities at the remaining primes ℓ (which are not necessarily independent from each other), we need a stronger version of Theorem 3.1.16, about the size of the Galois group of the field obtained by adjoining all the torsion points of E to $\mathbb{Q}$.

For any positive integer n, let $\rho_{E,n}$ denote the injective group homomorphism

$$\rho_{E,n} : \mathrm{Gal}\left(\mathbb{Q}\left(E[n]\right)/\mathbb{Q}\right) \to \mathrm{GL}_2\left(\mathbb{Z}/n\mathbb{Z}\right),$$

and let $G_E(n)$ denote the image of $\rho_{E,n}$ inside $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$. Taking the inverse limit of the $\rho_{E,n}$ over positive integers n (with a chosen compatible basis), we obtain a continuous group homomorphism

$$\rho_E : G_{\mathbb{Q}} \to \mathrm{GL}_2(\hat{\mathbb{Z}}),$$

where $\hat{\mathbb{Z}} = \varprojlim \mathbb{Z}/n\mathbb{Z}$, and $G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

Theorem 3.1.17. *(Serre, [Se2]) Let $E/\mathbb{Q}$ be an elliptic curve without complex multiplication. Then we have that*

$$[\mathrm{GL}_2(\hat{\mathbb{Z}}) : \rho_E(G_{\mathbb{Q}})] < \infty.$$

From Theorem 3.1.17, we have that there exist positive integers m such that, if

$$\pi : \mathrm{GL}_2(\hat{\mathbb{Z}}) \longrightarrow \mathrm{GL}_2\left(\mathbb{Z}/m\mathbb{Z}\right)$$

is the natural projection, then we have that

$$\rho_E\left(G_{\mathbb{Q}}\right) = \pi^{-1}\left(G_E(m)\right). \tag{3.1}$$

That is, $\rho_E\left(G_{\mathbb{Q}}\right)$ is the full inverse image of $G_E(m)$.

Remark 3.1.18. Let $E/\mathbb{Q}$ be an elliptic curve without complex multiplication. We define M_E to be the smallest positive integer m such that (3.1) holds. Then it follows from (3.1) that M_E has the following three properties:
1. If $(n, M_E) = 1$, then $G_E(n) = \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$,
2. If $(n, M_E) = (n, m) = 1$, then $G_E(mn) \simeq G_E(m) \times G_E(n)$,
3. If $M_E \mid m$, then $G_E(m) \subseteq \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$ is the full inverse image of $G_E(M_E) \subseteq \mathrm{GL}_2(\mathbb{Z}/M_E\mathbb{Z})$ under the projection map.

Thus, the probabilities will be independent for a prime $\ell \nmid M_E$ and at M_E by the three properties above.

The following proposition given in Serre [Se1, IV-4,IV-5] allows us to interpret the size of the group of points on the elliptic curve over $\mathbb{F}_p$ in terms of the Frobenius automorphisms, which we denote by σ_p in $\mathrm{Gal}(\mathbb{Q}(E[n])/\mathbb{Q})$ for an unramified prime p. We have that σ_p is the element of the Galois group which projects to the generator of the local Galois group at p.

Proposition 3.1.19. *(Serre, [Se1, IV-4,IV-5]) Let n be a positive integer and assume*

that p is a prime of good reduction which does not divide n. Then p is unramified in $\mathbb{Q}(E[n])$ and for any Frobenius automorphism $\sigma_p \in \mathrm{Gal}(\mathbb{Q}(E[n])/\mathbb{Q})$ we have that

$$\mathrm{tr}(\sigma_p) \equiv a_p(E) \pmod{n} \quad \text{and} \quad \det(\sigma_p) \equiv p \pmod{n}.$$

This gives us a model for the local probabilities since the Frobenius elements are equidistributed in conjugacy classes of the Galois group by the Cebotarev Density Theorem.

Hence, for the Lang-Trotter conjecture, for a prime $\ell \nmid M_E$ we have that

$$\begin{aligned}\mathrm{Prob}\left(a_p(E) \equiv t \pmod{\ell}\right) =& \frac{\#\left\{g \in \mathrm{GL}_2(\mathbb{F}_\ell) \mid \mathrm{tr}(g) \equiv t \pmod{\ell}\right\}}{\#\mathrm{GL}_2(\mathbb{F}_\ell)} \\ =& \begin{cases} \frac{\ell^2-\ell-1}{(\ell-1)^2(\ell+1)} & \text{if } \ell \nmid t, \\ \frac{\ell}{\ell^2-1} & \text{if } \ell \mid t. \end{cases}\end{aligned}$$

This leads to the following conjecture.

Conjecture 3.1.20. *(**Lang-Trotter**) Let $E/\mathbb{Q}$ be an elliptic curve without complex multiplication. Then we have that*

$$\pi_{E,t}^{\mathrm{LT}}(X) = \#\{p \leq X : a_p(E) = t\} \sim C_{E,t}^{\mathrm{LT}} \frac{\sqrt{X}}{\log X}$$

where

$$C_{E,t}^{\mathrm{LT}} = \frac{2}{\pi} \frac{M_E |C(M_E)|}{|G_E(M_E)|} \prod_{\substack{\ell \nmid M_E \\ \ell \mid t}} \left(1 - \frac{1}{\ell^2}\right)^{-1} \prod_{\substack{\ell \nmid M_E \\ \ell \nmid t}} \frac{\ell(\ell^2-\ell-1)}{(\ell-1)(\ell^2-1)},$$

and

$$C(M_E) = \left\{g \in G_E(M_E) \mid \mathrm{tr}(g) \equiv t \pmod{M_E}\right\}.$$

We note that the factor $\dfrac{2}{\pi}$ in the Lang-Trotter Conjecture comes from the Sato-Tate distribution appearing in the following conjecture, recently proven for elliptic curves over totally real fields which have multiplicative reduction at some prime by Harris, Shepherd-

Barron and Taylor [HSBT].

Conjecture 3.1.21. *(**Sato-Tate Conjecture**) Let $E/\mathbb{Q}$ be an elliptic curve without complex multiplication and let θ_p be a solution to the equation*

$$p + 1 - \#E_p(\mathbb{F}_p) = 2\sqrt{p}\cos\theta + p \quad (0 \leq \theta_p \leq \pi).$$

Then for every two real numbers α, β for which $0 \leq \alpha < \beta \leq \pi$ as $X \to \infty$ we have that

$$\frac{\#\{p \leq X : \alpha \leq \theta_p \leq \beta\}}{\#\{p \leq X\}} \sim \frac{2}{\pi}\int_{\alpha}^{\beta} \sin^2\theta d\theta.$$

Let

$$\mathcal{C} := \mathcal{C}(A, B) = \{E_{a,b} : Y^2 = X^3 + aX + b, a, b \in \mathbb{Z}, |a| \leq A, |b| \leq B\},$$

It was proven by Fouvry and Murty [FoMu] (for $t = 0$) and David and Pappalardi [DaPa] (for any integer t) that the Lang-Trotter conjecture holds on average, with the predicted constant, namely that

$$\frac{1}{4AB}\sum_{E \in \mathcal{C}} \pi^{\mathrm{LT}}_{E(a,b),t} \sim C^{\mathrm{LT}}_t \frac{\sqrt{X}}{\log X},$$

where

$$C^{\mathrm{LT}}_t = \frac{2}{\pi}\prod_{\ell | t}\left(1 - \frac{1}{\ell^2}\right)^{-1}\prod_{\ell \nmid t}\frac{\ell(\ell^2 - \ell - 1)}{(\ell - 1)(\ell^2 - 1)}$$

is the average of the Lang-Trotter constants of Conjecture 3.1.20 as proven by Jones in [Jon1]. This holds for A, B big enough, and the "trivial length of the average" is $A, B > X^{1+\epsilon}$ for some $\epsilon > 0$ in this case. The shorter length $A, B > X^{\frac{1}{2}+\epsilon}, AB > X^{\frac{3}{2}+\epsilon}$ obtained by Fouvry and Murty was improved to

$$A, B > (\log X)^{60+\epsilon} \quad \text{and} \quad X^{\frac{3}{2}}(\log X)^{10+\epsilon} < AB < e^{X^{\frac{1}{8}-\epsilon}}$$

by Baier [Ba2]. The additional condition $AB < e^{X^{\frac{1}{8}-\epsilon}}$ is not a limiting constraint since

we are mainly interested in averages for small values of A and B.

For the Koblitz conjecture, for a prime $\ell \nmid M_E$ we have that

$$\begin{aligned}\text{Prob}\left(\ell \nmid p+1-a_p(E)\right) &= \frac{\#\left\{g \in \mathrm{GL}_2(\mathbb{F}_\ell) \mid \ell \nmid \det(g)+1-\mathrm{tr}(g)\right\}}{\#\mathrm{GL}_2(\mathbb{F}_\ell)} \\ &= \frac{\ell^4-2\ell^3-\ell^2+3\ell}{\ell(\ell-1)^2(\ell+1)},\end{aligned}$$

which leads to the following conjecture of Koblitz [Kob], as modified by Zywina [Zyw].

Conjecture 3.1.22. *(**Koblitz conjecture**) Let $E/\mathbb{Q}$ be an elliptic curve without complex multiplication and let M_E be the smallest positive integer m such that* (3.1) *holds. Then,*

$$\begin{aligned}\pi_E^{\text{twin}}(X) =& \#\{p \le X : \#E(\mathbb{F}_p) = p+1-a_p(E) \text{ is prime}\} \\ \sim& C_E^{\text{twin}} \frac{X}{\log^2 X},\end{aligned}$$

where

$$C_E^{\text{twin}} = \frac{M_E|C(M_E)|}{\varphi(M_E)|G_E(M_E)|} \prod_{\ell \nmid M_E} \frac{\ell(\ell^3-2\ell^2-\ell+3)}{(\ell-1)^3(\ell+1)},$$

and

$$C(M_E) = \left\{g \in G_E(M_E) \mid (\det(g)+1-\mathrm{tr}(g), M_E) = 1\right\}.$$

Balog, Cojocaru and David [BCD] proved that the Koblitz Conjecture is true on average with $A, B \ge X^\epsilon$ and $AB \ge X^{1+\epsilon}$, with the predicted constant, namely that

$$\frac{1}{|\mathcal{C}|} \sum_{E \in \mathcal{C}} \pi_E^{\text{twin}}(X) \sim C^{\text{twin}} \frac{\sqrt{X}}{\log X},$$

where

$$C^{\text{twin}} = \prod_{\ell} \frac{\ell^4-2\ell^3-\ell^2+3\ell}{(\ell-1)^3(\ell+1)}.$$

We now return to the question of amicable pairs and aliquot cycles. In the amicable pairs case we need to consider $\text{Prob}(p+1-a_p(E) = q \text{ and } q+1-a_q(E) = p)$, so we will use the direct product $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z}) \times \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$. Then as suggested by Proposition 3.1.19

for a prime $\ell \nmid M_E$, we have the model

$$\begin{aligned}
&\text{Prob}\left(p+1-a_p(E) \equiv q \pmod{\ell} \text{ and } q+1-a_q(E) \equiv p \pmod{\ell}\right) \\
=&\frac{1}{|\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})^2|} \cdot \#\Bigg\{(g_1,g_2) \in \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})^2 \mid \det(g_1)+1-\mathrm{tr}(g_1) \equiv \det(g_2) \pmod{\ell} \\
&\qquad\qquad \text{and } \det(g_2)+1-\mathrm{tr}(g_2) \equiv \det(g_2) \pmod{\ell}\Bigg\} \\
=&\frac{\ell^4-2\ell^3-2\ell^2+3\ell+3}{(\ell^2-1)^2(\ell-1)^2},
\end{aligned}$$

as computed by Jones [Jon2]. Let $\phi(x) = \frac{2}{\pi}\sqrt{1-x^2}$ be the Sato-Tate measure, which is the density function of the random variable

$$\sum_{i=1}^{L} \frac{a_{p_i}(E)}{2\sqrt{p_i}},$$

coming from the Sato-Tate Conjecture, Conjecture 3.1.21. Now we denote by $\phi_L(x) := \phi * \phi * \cdots * \phi$ the L-fold convolution of ϕ with itself.

Conjecture 3.1.23. *(Jones, [Jon2]) Let $E/\mathbb{Q}$ be an elliptic curve without complex multiplication. Then,*

$$\pi_{E,2}(X) \sim C_{E,2}\frac{\sqrt{X}}{\log^2 X},$$

where

$$C_{E,2} = \frac{8}{3\pi^2}\frac{M_E^2|C(M_E)|}{|G_E(M_E)^2|}\prod_{\ell \nmid M_E}\frac{\ell^2(\ell^4-2\ell^3-2\ell^2+3\ell+3)}{(\ell^2-1)^2(\ell-1)^2}$$

and

$$\begin{aligned}
C(M_E) = \Bigg\{&(g_1,g_2) \in G_E(M_E)^2 \mid \det(g_1)+1-\mathrm{tr}(g_1) \equiv \det(g_2) \pmod{M_E}, \\
&\det(g_2)+1-\mathrm{tr}(g_2) \equiv \det(g_1) \pmod{M_E}\Bigg\}.
\end{aligned}$$

Finally, we state the general conjecture of Jones [Jon2] for $\pi_{E,L}(X)$, for any integer

$L \geq 2$. We first set some notation. For any integer $L \geq 2$ and any subgroup $G \subseteq \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$, we define

$$\mathrm{G}^L_{\mathrm{ali-cycle}} := \{(g_1, \ldots, g_L) \in \mathrm{G}^L \mid \det(g_{i+1}) = \det(g_i) + 1 - \mathrm{tr}(g_i) \text{ for } 1 \leq i \leq L\}.$$

Then we have that Proposition 3.1.19 suggests that, for $(n, M_E) = 1$, we have that

$$\mathrm{Prob}\Big(\text{For all } i \in \mathbb{Z}/L\mathbb{Z},\ \det(g_{i+1}) \equiv \det(g_i) + 1 - \mathrm{tr}(g_i) \pmod{n}\Big) = \frac{G_E(n)^L_{\mathrm{ali-cycle}}}{G_E(n)^L},$$

where we recall that $G_E(n)$ is the image of $\mathrm{Gal}(\mathbb{Q}(E[n])/\mathbb{Q})$ in $\mathrm{Gal}_2(\mathbb{Z}/n\mathbb{Z})$. Hence, we have the general conjecture of Jones [Jon2] for $\pi_{E,L}(X)$.

Conjecture 3.1.24. *(Jones, [Jon2]) Let $E/\mathbb{Q}$ be an elliptic curve without complex multiplication. Then,*

$$\pi_{E,L}(X) \sim C_{E,L} \frac{\sqrt{X}}{\log^L X},$$

where

$$C_{E,L} = \frac{\phi_L(0)}{L} \frac{M_E^L |G_E(M_E)^L_{\mathrm{ali-cycle}}|}{|G_E(M_E)^L|} \prod_{\ell \nmid M_E} \frac{\ell^L |\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})^L_{\mathrm{ali-cycle}}|}{|\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})^L|}.$$

This concludes the section on previous work in the study of amicable pairs and aliquot cycles of elliptic curves.

3.2 The average number of aliquot cycles

In this section we will consider the average of $\pi_{E,L}(X)$ for a family of elliptic curves. We begin by finding the trivial upper bound and trivial length of the average as an initial goal. We then obtain the conjectured upper bound for the average number of aliquot cycles using technical results that we will prove in Chapter 4 and 5.

The family we will consider will be the set

$$\mathcal{C} := \mathcal{C}(A, B) = \{E_{a,b} : y^2 = X^3 + aX + b, a, b \in \mathbb{Z}, |a| \leq A, |b| \leq B\}$$

which is a two parameter family of elliptic curves with nonzero discriminant. We have that the size of the family is

$$|\mathcal{C}| = \sum_{\substack{|a|\leq A \\ |b|\leq B}} 1 = 4AB + O(A + B + 1).$$

For a prime p_i and an elliptic curve $E \in \mathcal{C}$, we will denote the number of points on the elliptic curve over $\mathbb{F}_{p_i}$ as $\#E_{a,b}(\mathbb{F}_{p_i})$.

To ease notation we give the following notational conventions. We define $P := (p_1, \ldots, p_L)$ to be a vector of L distinct primes and we define the smallest prime in the vector to be $p := p_{L+1} := p_1$. For $1 \leq i \leq L-1$, from Theorem 2.1.20, we denote the limits of the Hasse interval as

$$p_i^- := p_i + 1 - 2\sqrt{p_i} < \#E_{p_i}(\mathbb{F}_{p_i}) < p_i^+ := p_i + 1 + 2\sqrt{p_i}.$$

For fixed a, b we define the following indicator function which determines if P is a normalized aliquot cycle of length L as follows

$$w(P) := \begin{cases} 1 & \text{if } \#E_{a,b}(\mathbb{F}_{p_i}) = p_{i+1} \text{ for } 1 \leq i \leq L, \\ 0 & \text{otherwise.} \end{cases}$$

We define the vectors $S := (s_1, \ldots, s_L)$ and $T := (t_1, \ldots, t_L)$ for $s_i, t_i \in \mathbb{F}_{p_i}$ with $1 \leq i \leq L$, which leads to the following similar indicator function

$$w(P, S, T) := \begin{cases} 1 & \text{if } \#E_{s_i,t_i}(\mathbb{F}_{p_i}) = p_{i+1} \text{ for } 1 \leq i \leq L, \\ 0 & \text{otherwise.} \end{cases} \tag{3.2}$$

We also define the following products of finite fields

$$\mathbb{F}(P) := \mathbb{F}_{p_1} \times \cdots \times \mathbb{F}_{p_L} \quad \text{and} \quad \mathbb{F}(P)^* := \mathbb{F}_{p_1}^* \times \cdots \times \mathbb{F}_{p_L}^*,$$

so that

$$\sum_{S,T\in\mathbb{F}(P)} 1 = \sum_{\substack{1\le s_1\le p_1\\ 1\le t_1\le p_1}} \cdots \sum_{\substack{1\le s_L\le p_L\\ 1\le t_L\le p_L}} 1 \quad \text{and} \quad \sum_{S,T\in\mathbb{F}(P)^*} 1 = \sum_{\substack{1\le s_1< p_1\\ 1\le t_1< p_1}} \cdots \sum_{\substack{1\le s_L< p_L\\ 1\le t_L< p_L}} 1.$$

Finally, for positive integers m and n we define

$$D(m,n) := (m+1-n)^2 - 4m = (n+1-m)^2 - 4n = D(n,m).$$

We have that

$$\begin{aligned}
&\frac{1}{|\mathcal{C}|}\sum_{E\in\mathcal{C}} \pi_{E,L}(X)\\
=&\frac{1}{|\mathcal{C}|}\sum_{E\in\mathcal{C}} \sum_{\substack{p\le X\\ p_i^-<p_{i+1}<p_i^+\\ 1\le i\le L-1}} w(P) = \frac{1}{|\mathcal{C}|}\sum_{\substack{p\le X\\ p_i^-<p_{i+1}<p_i^+\\ 1\le i\le L-1}} \sum_{E\in\mathcal{C}} w(P) \qquad (3.3)\\
=&\frac{1}{|\mathcal{C}|}\sum_{\substack{p\le X\\ p_i^-<p_{i+1}<p_i^+\\ 1\le i\le L-1}} \sum_{S,T\in\mathbb{F}(P)} w(P,S,T) \sum_{\substack{|a|\le A,|b|\le B\\ a\equiv s_i \pmod{p_i}\\ b\equiv t_i \pmod{p_i}\\ 1\le i\le L}} 1.\\
=&\frac{1}{|\mathcal{C}|}\sum_{\substack{p\le X\\ p_i^-<p_{i+1}<p_i^+\\ 1\le i\le L-1}} \sum_{S,T\in\mathbb{F}(P)} w(P,S,T)\left(\frac{2A}{p_1\cdots p_L}+O(1)\right)\left(\frac{2B}{p_1\cdots p_L}+O(1)\right)\\
=&\frac{4AB}{|\mathcal{C}|}\sum_{\substack{p\le X\\ p_i^-<p_{i+1}<p_i^+\\ 1\le i\le L-1}} \sum_{S,T\in\mathbb{F}(P)} \frac{w(P,S,T)}{p_1^2\cdots p_L^2} + O\Bigg(\frac{(B+A)}{|\mathcal{C}|}\sum_{\substack{p\le X\\ p_i^-<p_{i+1}<p_i^+\\ 1\le i\le L-1}} \sum_{S,T\in\mathbb{F}(P)} \frac{w(P,S,T)}{p_1\cdots p_L}\\
&+\frac{1}{|\mathcal{C}|}\sum_{\substack{p\le X\\ p_i^-<p_{i+1}<p_i^+\\ 1\le i\le L-1}} \sum_{S,T\in\mathbb{F}(P)} w(P,S,T)\Bigg), \qquad (3.4)
\end{aligned}$$

where

$$\sum_{S,T\in\mathbb{F}(P)} w(P,S,T) = \sum_{\substack{1\le s_1,t_1\le p_1\\ \#E_{s_1,t_1}(\mathbb{F}_{p_1})=p_2}} \cdots \sum_{\substack{1\le s_L,t_L\le p_L\\ \#E_{s_L,t_L}(\mathbb{F}_{p_L})=p_1}} 1. \qquad (3.5)$$

For $1\le i\le L$ the sums in (3.5) over s_i and t_i can be changed to a sum over isomorphism

classes which we denote by $\overline{E}_{s_i,t_i}$ and we have that

$$\sum_{\substack{1\le s_i,t_i\le p_i\\ \#E_{s_i,t_i}(\mathbb{F}_{p_i})=p_{i+1}}} 1 = \sum_{\substack{\overline{E}_{s_i,t_i}\in\mathbb{F}_{p_i}\\ p_i+1-a_{p_i}(\overline{E}_{s_i,t_i})=p_{i+1}}} \frac{p_i-1}{\#\mathrm{Aut}(\overline{\mathrm{E}}_{\mathrm{s_i,t_i}}(\mathbb{F}_{\mathrm{p_i}}))}$$

$$= (p_i-1)H(D((p_i+1-p_{i+1})^2-4p_i)), \tag{3.6}$$

by Deuring's Theorem, Theorem 2.1.27. Using the bounds for a Dirichlet character, χ of modulus d that $L(1,\chi_d)\ll \log d$ and by the analytic class number formula, Theorem 2.2.25 for $1\le i\le L$, we deduce that

$$\begin{aligned} H(D(p_i,p_{i+1})) &= \sum_{\substack{f^2\mid D(p_i,p_{i+1})\\ \frac{D(p_i,p_{i+1})}{f^2}\equiv 0,1 \pmod 4}} \frac{\sqrt{D(p_i,p_{i+1})}}{2\pi f} L\left(1,\left(\frac{D(p_i,p_{i+1})/f^2}{\cdot}\right)\right)\\ &\ll \sqrt{D(p_i,p_{i+1})}\log(p_i)\sum_{f\mid D(p_i,p_{i+1})}\frac{1}{f} \ll \sqrt{p_i}\log p_i(\log\log D(p_i,p_{i+1}))\\ &\ll \sqrt{p}\log p\log\log p, \end{aligned} \tag{3.7}$$

since $p_i = p+O(\sqrt{p})$.

Thus, from (3.6) and (3.7) we have that the main term in (3.4) is bounded by

$$\begin{aligned} &\ll_L \frac{AB}{|\mathcal{C}|}\sum_{p\le X}\frac{1}{p^L}\sum_{\substack{p_i^-<p_{i+1}<p_i^+\\ 1\le i\le L-1}}\prod_{j=1}^{L}H(D(p_j,p_{j+1}))\\ &\ll_L \left(1+O\left(\frac{1}{A}+\frac{1}{B}+\frac{1}{AB}\right)\right)\sum_{p\le X}\frac{1}{p^L}\frac{p^{\frac{L-1}{2}}}{(\log p)^{L-1}}p^{\frac{L}{2}}(\log p)^L(\log\log p)^L\\ &\ll_L \sum_{p\le X}\frac{\log p(\log\log p)^L}{\sqrt{p}} \ll_L \sqrt{X}(\log\log X)^L. \end{aligned} \tag{3.8}$$

Similarly, the error term in (3.4) becomes

$$\begin{aligned}&\ll_L \left(\frac{1}{A}+\frac{1}{B}\right)\sum_{p\leq X} p^{L-\frac{1}{2}}\log p(\log\log p)^L + \frac{1}{AB}\sum_{p\leq X} p^{2L-\frac{1}{2}}\log p(\log\log p)^L\\ &\ll_L \left(\frac{1}{A}+\frac{1}{B}\right)X^{L+\frac{1}{2}}(\log\log X)^L + \frac{X^{2L+\frac{1}{2}}(\log\log X)^L}{AB}. \end{aligned} \tag{3.9}$$

Hence, from (3.9) to obtain the correct upper bound for the average we will need

$$A, B > X^L(\log X)^L(\log\log X)^L \quad \text{and} \quad AB > X^{2L}(\log X)^L(\log\log X)^L,$$

whereas $\pi_{E,L}$ only considers primes of size at most X. Also, we see that using the trivial bound for $H(D(p_i, p_{i+1}))$ in (3.4) does not give the correct order of magnitude for the main term in (3.8). Therefore, we will need other techniques which we develop in Chapter 4.

We now rewrite (3.3) as a sum over isomrphism classes and from Proposition 2.1.23 and the definition of an isomorphism of an elliptic curve we have that

$$\begin{aligned}\frac{1}{|\mathcal{C}|}\sum_{E\in\mathcal{C}}\pi_{E,L}(X) =& \frac{1}{|\mathcal{C}|}\sum_{\substack{p\leq X\\ p_i^-<p_{i+1}<p_i^+\\ 1\leq i\leq L-1}}\sum_{S,T\in\mathbb{F}(P)}\frac{\#\mathrm{Aut}(\mathrm{E}_{\mathrm{s}_1,\mathrm{t}_1})\cdots\#\mathrm{Aut}(\mathrm{E}_{\mathrm{s}_\mathrm{L},\mathrm{t}_\mathrm{L}})}{(p_1-1)\cdots(p_L-1)}\\ &\times w(P,S,T)R(P,S,T), \end{aligned} \tag{3.10}$$

where $R(P,S,T)$ is the number of integers $|a|\leq A, |b|\leq B$ such that there exist $U := (u_1,\ldots,u_L)\in\mathbb{F}(P)^*$ satisfying

$$a\equiv s_i u_i^4 \pmod{p_i}, \quad b\equiv t_i u_i^6 \pmod{p_i} \quad \text{for } 1\leq i\leq L.$$

Since we are summing over more congruence classes in (3.10) than in (3.4) we are able to take A, B to be much smaller and we obtain the following theorem.

Theorem 3.2.1. *Fix an integer $L\geq 2$, let $E/\mathbb{Q}$ be an elliptic curve, let $\epsilon>0$ and let k*

be any positive integer. Then for our family of elliptic curves $\mathcal{C}$ we have that

$$\frac{1}{|\mathcal{C}|}\sum_{E\in\mathcal{C}}\pi_{E,L}(X)=\left\{\sum_{p\leq X}\frac{1}{p^L}\sum_{\substack{p_i^-<p_{i+1}<p_i^+\\1\leq i\leq L-1}}\prod_{j=1}^{L}H(D(p_j,p_{j+1}))\right\}\left(1+O\left(\frac{1}{X^\epsilon}\right)\right) \tag{3.11}$$

Proof. From Corollary 2.1.22 we have a criterion for determining the size of $\mathrm{Aut}(\mathrm{E}_{\mathrm{s_i,t_i}})$ so we split up the sum in (3.10) into two cases, $s_it_i\not\equiv 0 \pmod{p_i}$ and $s_it_i\equiv 0 \pmod{p_i}$. Then we have that (3.10) becomes

$$\begin{aligned}\frac{1}{|\mathcal{C}|}\sum_{E\in\mathcal{C}}\pi_{E,L}(X)=&\frac{2^L}{|\mathcal{C}|}\sum_{\substack{p\leq X\\p_i^-<p_{i+1}<p_i^+\\1\leq i\leq L-1}}\sum_{S,T\in\mathbb{F}(P)^*}\frac{w(P,S,T)R(P,S,T)}{(p_1-1)\cdots(p_L-1)}\\&+\frac{1}{|\mathcal{C}|}\sum_{\substack{p\leq X\\p_i^-<p_{i+1}<p_i^+\\1\leq i\leq L-1}}\sum_{\substack{S,T\in\mathbb{F}(P)\\s_it_i\equiv 0 \pmod{p_i}}}\frac{\#\mathrm{Aut}(\mathrm{E}_{\mathrm{s_1,t_1}})\cdots\#\mathrm{Aut}(\mathrm{E}_{\mathrm{s_L,t_L}})}{(p_1-1)\cdots(p_L-1)}\\&\times w(P,S,T)R(P,S,T).\end{aligned} \tag{3.12}$$

We first consider the first sum in (3.12), which we express as

$$\begin{aligned}&\frac{2^L}{|\mathcal{C}|}\sum_{\substack{p\leq X\\p_i^-<p_{i+1}<p_i^+\\1\leq i\leq L-1}}\sum_{S,T\in\mathbb{F}(P)^*}\frac{w(P,S,T)R(P,S,T)}{(p_1-1)\cdots(p_L-1)}\\=&\frac{4AB}{|\mathcal{C}|}\sum_{\substack{p\leq X\\p_i^-<p_{i+1}<p_i^+\\1\leq i\leq L-1}}\prod_{j=1}^{L}\frac{1}{p_j(p_j-1)}\sum_{S,T\in\mathbb{F}(P)^*}w(P,S,T)\\+&\frac{2^L}{|\mathcal{C}|}\sum_{\substack{p\leq X\\p_i^-<p_{i+1}<p_i^+\\1\leq i\leq L-1}}\prod_{j=1}^{L}\frac{1}{(p_j-1)}\sum_{S,T\in\mathbb{F}(P)^*}w(P,S,T)\left(R(P,S,T)-\frac{4AB}{2^Lp_1\cdots p_L}\right).\end{aligned} \tag{3.13}$$

The first term in (3.13) contributes to the main term, but we will need the following technical lemma to bound the second term in (3.13), which we prove in Chapter 5.

Lemma 3.2.2. *Fix an integer $L\geq 2$, let $E/\mathbb{Q}$ be an elliptic curve, let $A,B>0$ then for*

any positive integer k, we have that as $X \to \infty$,

$$\sum_{\substack{p\le X\\ p_i^-<p_{i+1}<p_i^+\\ 1\le i\le L-1}} \frac{1}{p_1\cdots p_L}\sum_{S,T\in\mathbb{F}(P)^*} w(P,S,T)\left(R(P,S,T)-\frac{AB}{2^{L-2}p_1\cdots p_L}\right)$$
$$\ll_{k,L} ABX^{\frac{1}{2}-\frac{1}{4k}}(\log X)^{\frac{L-1}{2k}}(\log\log X)^L\log^{\frac{k^2-1}{2k}} AB$$
$$+(A\sqrt{B}+B\sqrt{A})X^{\frac{1}{2}+\frac{3L-1}{4k}}(\log X)^{\frac{k^2+L-1}{2k}}(\log\log X)^L+\sqrt{AB}X^{\frac{3L+2}{4}}(\log X)^{3-L}.$$

Thus, from Lemma 3.2.2 we have that for any positive integer k, the second sum in (3.13) becomes

$$\frac{2^L}{|\mathcal{C}|}\sum_{\substack{p\le X\\ p_i^-<p_{i+1}<p_i^+\\ 1\le i\le L-1}} \frac{1}{(p_1-1)\cdots(p_L-1)}\sum_{S,T\in\mathbb{F}(P)^*} w(P,S,T)\left(R(P,S,T)-\frac{4AB}{2^Lp_1\cdots p_L}\right)$$
$$\ll_L \frac{1}{|\mathcal{C}|}\sum_{\substack{p\le X\\ p_i^-<p_{i+1}<p_i^+\\ 1\le i\le L-1}} \frac{1}{p_1\cdots p_L}\sum_{S,T\in\mathbb{F}(P)^*} w(P,S,T)\left(R(P,S,T)-\frac{4AB}{2^Lp_1\cdots p_L}\right)$$
$$\ll_{L,k} X^{\frac{1}{2}-\frac{1}{4k}}(\log X)^{\frac{L-1}{2k}}(\log\log X)^L\log^{\frac{k^2-1}{2k}} AB+\frac{1}{\sqrt{AB}}X^{\frac{3L+2}{4}}(\log X)^{3-L}$$
$$+\left(\frac{1}{\sqrt{B}}+\frac{1}{\sqrt{A}}\right)X^{\frac{1}{2}+\frac{3L-1}{4k}}(\log X)^{\frac{k^2+L-1}{2k}}(\log\log X)^L. \tag{3.14}$$

We now consider the first term in (3.13),

$$\frac{4AB}{|\mathcal{C}|}\sum_{\substack{p\le X\\ p_i^-<p_{i+1}<p_i^+\\ 1\le i\le L-1}}\prod_{j=1}^{L}\frac{1}{p_j(p_j-1)}\sum_{S,T\in\mathbb{F}(P)^*} w(P,S,T)$$
$$=\frac{4AB}{|\mathcal{C}|}\sum_{\substack{p\le X\\ p_i^-<p_{i+1}<p_i^+\\ 1\le i\le L-1}}\frac{1}{p_1^2\cdots p_L^2}\sum_{S,T\in\mathbb{F}(P)^*} w(P,S,T)\left(1+O\left(\frac{1}{p}\right)\right). \tag{3.15}$$

As in the trivial case we first consider the sum

$$\sum_{S,T\in\mathbb{F}(P)^*} w(P,S,T) = \sum_{\substack{1\le s_1,t_1<p_1\\ \#E_{s_1,t_1}(\mathbb{F}_{p_1})=p_2}} \cdots \sum_{\substack{1\le s_L,t_L<p_L\\ \#E_{s_L,t_L}(\mathbb{F}_{p_L})=p_1}} 1. \tag{3.16}$$

For $1 \le i \le L$ the sums in (3.16) over s_i and t_i can be changed to a sum over isomorphism classes and we have that

$$\begin{aligned}\sum_{\substack{1\le s_i,t_i<p_i\\ \#E_{s_i,t_i}(\mathbb{F}_{p_i})=p_{i+1}}} 1 &= \sum_{\substack{1\le s_i,t_i\le p_i\\ \#E_{s_i,t_i}(\mathbb{F}_{p_i})=p_{i+1}}} 1 - \sum_{\substack{1\le s_i\le p_i\\ \#E_{s_i,0}(\mathbb{F}_{p_i})=p_{i+1}}} 1 - \sum_{\substack{1\le t_i\le p_i\\ \#E_{0,t_i}(\mathbb{F}_{p_i})=p_{i+1}}} 1\\ &= \sum_{\substack{\overline{E}_{s_i,t_i}\in\mathbb{F}_{p_i}\\ p_i+1-a_{p_i}(\overline{E}_{s_i,t_i})=p_{i+1}}} \frac{p_i-1}{\#\mathrm{Aut}(\overline{\mathrm{E}}_{\mathrm{s_i,t_i}}(\mathbb{F}_{\mathrm{p_i}}))} + O(p_i)\\ &= (p_i-1)H(D((p_i+1-p_{i+1})^2-4p_i)) + O(p), \end{aligned} \tag{3.17}$$

by Deuring's Theorem, Theorem 2.1.27 and since $p_i = p + O(\sqrt{p})$.

Hence, from (3.7) and (3.17) we have that

$$\begin{aligned}\sum_{S,T\in\mathbb{F}(P)^*} w(P,S,T) =& \prod_{i=1}^{L} ((p_i-1)H(D(p_i,p_{i+1})) + O(p_i))\\ =& p^L \prod_{i=1}^{L} H(D(p_i,p_{i+1})) + O\left(p^{\frac{3L-1}{2}}(\log p)^L(\log\log p)^L\right), \end{aligned} \tag{3.18}$$

and therefore from (3.18) we have that

$$\begin{aligned}
&\sum_{\substack{p\le X\\ p_i^-<p_{i+1}<p_i^+\\ 1\le i\le L-1}} \frac{1}{p_1^2\cdots p_L^2}\sum_{S,T\in\mathbb{F}(P)^*} w(P,S,T)\\
=&\sum_{p\le X}\left(\frac{1}{p^{2L}}+O\left(\frac{1}{p^{2L+\frac{1}{2}}}\right)\right)\left(p^L\sum_{\substack{p_i^-<p_{i+1}<p_i^+\\ 1\le i\le L-1}}\prod_{j=1}^{L}H(D(p_j,p_{j+1}))\right.\\
&\left.+O\left(p^{\frac{3L-1}{2}}(\log p)^L(\log\log p)^L\cdot\frac{p^{\frac{L-1}{2}}}{(\log p)^{L-1}}\right)\right)\\
=&\sum_{p\le X}\frac{1}{p^L}\sum_{\substack{p_i^-<p_{i+1}<p_i^+\\ 1\le i\le L-1}}\prod_{j=1}^{L}H(D(p_j,p_{j+1}))+O\left((\log X)(\log\log X)^{L+1}\right). \qquad (3.19)
\end{aligned}$$

Combining (3.15) and (3.19) gives

$$\begin{aligned}
&\frac{4AB}{|\mathcal{C}|}\sum_{\substack{p\le X\\ p_i^-<p_{i+1}<p_i^+\\ 1\le i\le L-1}} \frac{1}{p_1^2\cdots p_L^2}\sum_{S,T\in\mathbb{F}(P)^*} w(P,S,T)\left(1+O\left(\frac{1}{p}\right)\right)\\
=&\frac{4AB}{|\mathcal{C}|}\sum_{p\le X}\frac{1}{p^L}\sum_{\substack{p_i^-<p_{i+1}<p_i^+\\ 1\le i\le L-1}}\prod_{j=1}^{L}H(D(p_j,p_{j+1}))+O_L\left(\frac{AB}{|\mathcal{C}|}\log X(\log\log X)^{L+1}\right)\\
=&\sum_{p\le X}\frac{1}{p^L}\sum_{\substack{p_i^-<p_{i+1}<p_i^+\\ 1\le i\le L-1}}\prod_{j=1}^{L}H(D(p_j,p_{j+1}))+O_L\Bigg(\left(\frac{1}{A}+\frac{1}{B}+\frac{1}{AB}\right)\\
&\times\sum_{p\le X}\frac{1}{p^L}\sum_{\substack{p_i^-<p_{i+1}<p_i^+\\ 1\le i\le L-1}}\prod_{j=1}^{L}H(D(p_j,p_{j+1}))+\log X(\log\log X)^{L+1}\Bigg). \qquad (3.20)
\end{aligned}$$

Note that in (3.20) we can write the main term as

$$\sum_{p\le X}\frac{1}{p^L}\prod_{i=1}^{L-2}\left(\sum_{p_i^-<p_{i+1}<p_i^+}H(D(p_i,p_{i+1}))\right)\sum_{p_{L-1}^-\le p_L\le p_{L-1}^+}H(D(p_L,p))H(D(p_L,p_{L-1})),$$

and thus we need to find upper bounds for the sums

$$\sum_{p_{L-1}^{-}\leq p_L\leq p_{L-1}^{+}} H(D(p_L,p))H(D(p_L,p_{L-1}))$$

and

$$\sum_{p_i^{-}\leq p_{i+1}\leq p_i^{+}} H(D(p_i,p_{i+1}))$$

in (3.19). We state the following technical propostions to bound the sums above, which is the primary focus of Chapter 4.

Proposition 3.2.3. *Fix primes $p,r>3$ not necessarily distinct and let q be a prime in the range $p^{-}\leq q\leq p^{+}$. Then we have that*

$$\sum_{p^{-}<q<p^{+}} H(D(p,q))H(D(r,q)) \ll \frac{p^{\frac{3}{2}}}{\log(p)}.$$

Proposition 3.2.4. *Let p,q be distinct primes in the range $p^{-}<q<p^{+}$. Then we have that*

$$\sum_{p^{-}<q<p^{+}} H(D(p,q)) \ll \frac{p}{\log(p)}.$$

We see that the first term in (3.20) gives the main term in (3.11) and by Proposition 3.2.3 and Proposition 3.2.4 we have that the error term in (3.20) is bounded by

$$\begin{aligned}
&\ll_L \left(\sum_{p\leq X}\frac{1}{p^L}\frac{p^{L-2}}{(\log p)^{L-2}}\frac{p^{\frac{3}{2}}}{\log p}\right)\left(\frac{1}{A}+\frac{1}{B}+\frac{1}{AB}\right)+\log X(\log\log X)^{L+1}\\
&\ll_L \left(\frac{1}{A}+\frac{1}{B}+\frac{1}{AB}\right)\sum_{p\leq X}\frac{1}{\sqrt{p}(\log p)^{L-1}}\\
&\ll_L \left(\frac{1}{A}+\frac{1}{B}+\frac{1}{AB}\right)\frac{\sqrt{X}}{\log X},
\end{aligned}$$

which is smaller than the third and fourth terms in the error terms in (3.14).

Thus, it remains to consider the second term in (3.12). Similarly to the treatment of

the average of the Lang-Trotter Conjecture by Baier [Ba2, Theorem 2.1] we have that

$$\frac{1}{|\mathcal{C}|}\sum_{\substack{p\leq X\\ p_i^-<p_{i+1}<p_i^+\\ 1\leq i\leq L-1}}\sum_{\substack{S,T\in\mathbb{F}(P)\\ s_it_i\equiv 0 \pmod{p_i}\\ 1\leq i\leq L}}\frac{\#\mathrm{Aut}(\mathrm{E}_{\mathrm{s}_1,\mathrm{t}_1})\cdots\#\mathrm{Aut}(\mathrm{E}_{\mathrm{s}_L,\mathrm{t}_L})}{(p_1-1)\cdots(p_L-1)}w(P,S,T)\sum_{\substack{|a|\leq A,|b|\leq B\\ U\in\mathbb{F}(P)^*\\ a\equiv s_iu_i^4 \pmod{p_i}\\ b\equiv t_iu_i^6 \pmod{p_i}\\ 1\leq i\leq L}}1$$

$$\ll_L\frac{1}{|\mathcal{C}|}\sum_{\substack{p\leq X\\ p_i^-<p_{i+1}<p_i^+\\ 1\leq i\leq L-1}}\sum_{\substack{|a|\leq A,|b|\leq B\\ ab\equiv 0 \pmod{p_1} \text{ or}\\ ab\equiv 0 \pmod{p_i}\\ \text{for } 2\leq i\leq L}}w(P). \tag{3.21}$$

If $ab\equiv 0 \pmod{p_j}$ then fixing p_j completely determines the other p_i for $1\leq i\neq j\leq L$ from $w(P)$. Hence, without loss of generality we can assume that $ab\equiv 0 \pmod{p_1}$ and we have that (3.21) is bounded by

$$\ll_L\frac{1}{|\mathcal{C}|}\sum_{\substack{|a|\leq A\\ |b|\leq B}}\sum_{\substack{p\leq X\\ p\mid ab}}w(P)$$

$$\ll_L\frac{1}{|\mathcal{C}|}\sum_{|a|\leq A,|b|\leq B}\tau(ab)\ll_L\frac{1}{|\mathcal{C}|}\sum_{n\leq AB}\tau^2(n)\ll_L\log^3(AB),$$

by Theorem 2.2.6. Thus we have that

$$\begin{aligned}\frac{1}{|\mathcal{C}|}\sum_{E\in\mathcal{C}}\pi_{E,L}(X)=&\sum_{p\leq x}\frac{1}{p^L}\sum_{\substack{p_i^-<p_{i+1}<p_i^+\\ 1\leq i\leq L-1}}\prod_{j=1}^{L}H(D(p_j,p_{j+1}))+O_{L,k}\Bigg(\log^3(AB)\\ &+X^{\frac{1}{2}-\frac{1}{4k}}(\log X)^{\frac{L-1}{2k}}(\log\log X)^L\log^{\frac{k^2-1}{2k}}AB+\frac{1}{\sqrt{AB}}X^{\frac{3L+2}{4}}(\log X)^{3-L}\\ &+\left(\frac{1}{\sqrt{B}}+\frac{1}{\sqrt{A}}\right)X^{\frac{1}{2}+\frac{3L-1}{4k}}(\log X)^{\frac{k^2+L-1}{2k}}(\log\log X)^L\Bigg),\end{aligned} \tag{3.22}$$

which completes the proof. □

From the results of Theorem 3.2.1, Proposition 3.2.3 and Proposition 3.2.4 we can now obtain the following theorem for the upper bound for the average number of aliquot cycles for a family of elliptic curves with a short length for the average.

Theorem 3.2.5. *Fix an integer $L \geq 2$ and let $\epsilon_L > 0$, let $E/\mathbb{Q}$ be an elliptic curve and let $\mathcal{C}$ be the family of elliptic curves defined above with*

$$A, B > X^{\epsilon_L} \quad \text{and} \quad X^{\frac{3L}{2}}(\log X)^6 < AB < e^{X^{\frac{1}{6}}\log^{\frac{-L}{3}} X},$$

then

$$\frac{1}{|\mathcal{C}|}\sum_{E\in\mathcal{C}} \pi_{E,L}(X) \ll_L \frac{\sqrt{X}}{(\log X)^L}.$$

Proof. We recall (3.22) below

$$\begin{aligned}\frac{1}{|\mathcal{C}|}\sum_{E\in\mathcal{C}} \pi_{E,L}(X) =& \sum_{p\leq x}\frac{1}{p^L}\sum_{\substack{p_i^- < p_{i+1} < p_i^+ \\ 1\leq i\leq L-1}}\prod_{j=1}^{L} H(D(p_j, p_{j+1})) + O_{L,k}\Bigg(\log^3(AB) \\ &+ X^{\frac{1}{2}-\frac{1}{4k}}(\log X)^{\frac{L-1}{2k}}(\log\log X)^L \log^{\frac{k^2-1}{2k}} AB + \frac{1}{\sqrt{AB}}X^{\frac{3L+2}{4}}(\log X)^{3-L} \\ &+ \left(\frac{1}{\sqrt{B}} + \frac{1}{\sqrt{A}}\right) X^{\frac{1}{2}+\frac{3L-1}{4k}}(\log X)^{\frac{k^2+L-1}{2k}}(\log\log X)^L\Bigg). \end{aligned} \tag{3.23}$$

From Proposition 3.2.3 and Proposition 3.2.4 we have by partial summation that the main term in (3.23) is

$$\sum_{p\leq X}\sum_{\substack{p_i^- < p_{i+1} < p_i^+ \\ 1\leq i\leq L-1}}\prod_{j=1}^{L} H(D(p_j, p_{j+1})) \ll_L \sum_{p\leq X}\frac{1}{\sqrt{p}(\log p)^{L-1}} \ll_L \frac{\sqrt{X}}{(\log X)^L}.$$

Now the first term in the error term of (3.23) is smaller than the main term if

$$AB < e^{X^{\frac{1}{6}}\log^{\frac{-L}{3}} X}.$$

The second term in the error term of (3.23) is smaller than the main term for any $k \geq 1$. The third term in the error term of (3.23) is smaller than the main term if

$$AB > X^{\frac{3L}{2}}(\log X)^6.$$

The fourth term in the error term of (3.23) is smaller than the main term if

$$A, B > X^{\frac{3L-1}{2k}} (\log X)^{\frac{k^2+L-1}{k}+2L} (\log\log X)^{2L},$$

since for every $\epsilon_L > 0$ we can find a positive integer k such that

$$\epsilon_L > \frac{3L-1}{2k},$$

which gives the result. □

Chapter 4

Bounds on sums of class numbers

4.1 Upper bounds on sums of class numbers

In the previous chapter we were led to consider the sum of class numbers over primes in a short interval of the form

$$\sum_{p_{L-1}^- < p_L < p_{L-1}^+} H(D(p_L, p))H(D(p_L, p_{L-1})) \tag{4.1}$$

and

$$\sum_{p_i^- < p_{i+1} < p_i^+} H(D(p_i, p_{i+1})), \tag{4.2}$$

for $1 \leq i \leq L-1$. The goal of this chapter is to obtain upper bounds for the sum of class numbers in (4.1) and (4.2) to prove Proposition 3.2.3 and Proposition 3.2.4.

Remark 4.1.1. Recently, David and Smith [DaSm1] have considered the average of the function

$$M_E(N) := \#\{p : \#E(\mathbb{F}_p) = N\},$$

for a family of elliptic curves where they show the upper bound

$$\frac{1}{|\mathcal{C}|} \sum_{E \in \mathcal{C}} M_E(N) \ll \frac{\log \log N}{\log N},$$

for

$$A, B \geq \sqrt{N} \log N \quad \text{and } AB \geq N^{\frac{3}{2}+\epsilon}$$

for some $\epsilon > 0$. This result was improved by Chandee, David, Koukoulopolous and Smith [CDKS] to give the upper bound

$$\frac{1}{|\mathcal{C}|} \sum_{E \in \mathcal{C}} M_E(N) \ll \frac{N}{\varphi(N) \log N},$$

using the fundamental lemma of the combinatorial sieve. Their question is similar to ours, however in their proof, they are led to consider a sum of class numbers, whereas in our case we consider a sum of a product of class numbers.

Proposition 4.1.2. *Fix primes $p, r > 3$ not necessarily distinct and let q be a prime in the range $p^- \leq q \leq p^+$. Then we have that*

$$\sum_{p^- < q < p^+} H(D(p,q)) H(D(r,q)) \ll \frac{p^{\frac{3}{2}}}{\log(p)}. \tag{4.3}$$

Proof. As in the proof of [CDKS, Proposition 4.1] we will require the use of the fundamental lemma of the combinatorial sieve, Lemma 2.2.28. We begin by using the analytic class number formula in Theorem 2.2.25 to relate the class number $H(D)$ to a quadratic Dirichlet L-function evaluated at one. So we have that

$$H(D) = \sum_{\substack{f^2 | D \\ \frac{D}{f^2} \equiv 0,1 \pmod 4}} \frac{\sqrt{D}}{2\pi f} L\left(1, \left(\frac{D/f^2}{\cdot}\right)\right).$$

Since $\frac{D}{f^2} \not\equiv 0 \pmod 4$ for $p, q > 3$ and $\frac{D}{f^2} \equiv 1 \pmod 4$ if and only if f is odd we have

that

$$\sum_{p^-<q<p^+} H(D(p,q))H(D(r,q)) = \sum_{p^-<q<p^+} \sum_{\substack{f_1^2|D(p,q)\\(f_1,2)=1}} \frac{\sqrt{|D(p,q)|}}{2\pi f_1} L\left(1, \left(\frac{D(p,q)/f_1^2}{\cdot}\right)\right) \times \sum_{\substack{f_2^2|D(r,q)\\(f_2,2)=1}} \frac{\sqrt{|D(r,q)|}}{2\pi f_2} L\left(1, \left(\frac{D(r,q)/f_2^2}{\cdot}\right)\right).$$

Since $q, r = p + O(\sqrt{p})$ we have that $D(p,q), D(r,q) \ll p$. With the goal of obtaining an upper bound we define the sum

$$S_1 := \sum_{p^-<q<p^+} \sum_{\substack{f_1^2|D(p,q)\\f_2^2|D(r,q)\\(f_1f_2,2)=1}} \frac{L\left(1, \left(\frac{D(p,q)/f_1^2}{\cdot}\right)\right) L\left(1, \left(\frac{D(r,q)/f_2^2}{\cdot}\right)\right)}{f_1 f_2}. \tag{4.4}$$

For any quadratic Dirichlet character χ and any prime ℓ we have that

$$\left(1+\frac{1}{\ell}\right)^{-1} \leq \left(1-\frac{\chi(\ell)}{\ell}\right)^{-1} \leq \left(1-\frac{1}{\ell}\right)^{-1},$$

for a prime ℓ. From the properties of the Euler φ-function, Proposition 2.2.4 we have that

$$\begin{aligned} L\left(1, \left(\frac{D(p,q)/f_1^2}{\cdot}\right)\right) &= \prod_{\ell} \left(1 - \left(\frac{D(p,q)/f_1^2}{\ell}\right)\frac{1}{\ell}\right)^{-1} \\ &\leq \prod_{\ell \nmid 2f_1} \left(1 - \frac{\left(\frac{D(p,q)}{\ell}\right)}{\ell}\right)^{-1} \prod_{\ell|2f_1} \left(1-\frac{1}{\ell}\right)^{-1} \\ &= \frac{2f_1}{\varphi(2f_1)} \prod_{\ell\nmid 2f_1} \left(1 - \left(\frac{D(p,q)}{\ell}\right)\frac{1}{\ell}\right)^{-1} \\ &\leq \frac{2f_1}{\varphi(f_1)} \prod_{\ell\nmid 2f_1} \left(1 - \frac{\left(\frac{(2f_1)^2 D(p,q)}{\ell}\right)}{\ell}\right)^{-1} \\ &\ll \frac{f_1}{\varphi(f_1)} L\left(1, \left(\frac{(2f_1)^2 D(p,q)}{\cdot}\right)\right), \end{aligned} \tag{4.5}$$

and similarly,

$$L\left(1,\left(\frac{D(r,q)/f_2^2}{\cdot}\right)\right) \ll \frac{f_2}{\varphi(f_2)} L\left(1,\left(\frac{(2f_2)^2 D(r,q)}{\cdot}\right)\right).$$

To ease notation for the remainder of this section we denote

$$\chi_1 := \left(\frac{(2f_1)^2 D(p,q)}{\cdot}\right) \quad \text{and} \quad \chi_2 := \left(\frac{(2f_2)^2 D(r,q)}{\cdot}\right).$$

Now we have that

$$\begin{aligned} S_1 &\ll \sum_{p^-<q<p^+} \sum_{\substack{f_1^2 | D(p,q) \\ f_2^2 | D(r,q) \\ (f_1 f_2, 2)=1}} \frac{L(1,\chi_1) L(1,\chi_2)}{\varphi(f_1)\varphi(f_2)} \\ &\ll \sum_{p^-<q<p^+} \sum_{\substack{f_1 | D(p,q) \\ f_2 | D(r,q) \\ (f_1 f_2, 2)=1}} \frac{L(1,\chi_1) L(1,\chi_2)}{\varphi(f_1)\varphi(f_2)}, \end{aligned} \tag{4.6}$$

since the sum on the RHS in (4.6) is longer than the sum in (4.4).

Since

$$\sum_{p^-<q<p^+} H(D(p,q))H(D(r,q)) \ll pS_1,$$

the remainder of the proof is now reduced to showing the upper bound

$$S_2 := \sum_{p^-<q<p^+} \sum_{\substack{f_1 | D(p,q) \\ f_2 | D(r,q) \\ (f_1 f_2, 2)=1}} \frac{L(1,\chi_1) L(1,\chi_2)}{\varphi(f_1)\varphi(f_2)} \ll \frac{\sqrt{p}}{\log p}. \tag{4.7}$$

Let S_2' denote the same sum on the LHS of (4.7) but with $L\left(1,\chi_i; z^{8\alpha^2}\right)$ in place of $L(1,\chi_i)$ for $i = 1, 2$, where we define $z := \log(p)$ for convenience and α is some parameter ≥ 10. We estimate the error term $R := S_2 - S_2'$ by applying the result of Granville and Soundararajan, Lemma 2.2.27 with $Q = 4p$ or $4r$ for $i = 1, 2$ respectively. Then we have that $0 \leq -D(p,q) \leq 4p$ and $0 \leq -D(r,q) \leq 4r$ for $q \in (p^-, p^+)$. So, if the

conductor of χ_i, which is the discriminant of $\mathbb{Q}(\sqrt{D(p,q)})$, does not belong to $\mathcal{E}_\alpha(4p)$ or if the conductor of χ_2, which is the discriminant of $\mathbb{Q}(\sqrt{D(r,q)})$, does not belong to $\mathcal{E}_\alpha(4r)$, we can approximate $L(1,\chi_i)$ very well by $L\left(1,\chi_i; z^{8\alpha^2}\right) \ll_\alpha \log z$ by Mertens' Theorem, Theorem 2.2.26; else, we use the trivial bound $L(1,\chi_i) \ll z$ for $i = 1, 2$ and bound the number of exceptions. This yields the estimate

$$\begin{aligned} R \ll_\alpha & \left(\frac{(\log z)^2}{z^\alpha} + \frac{\log^2 z}{z^{2\alpha}}\right) \sum_{\substack{p^-<q<p^+ \\ \operatorname{disc}(\mathbb{Q}(\sqrt{D(p,q)}))\notin\mathcal{E}(4p) \\ \operatorname{disc}(\mathbb{Q}(\sqrt{D(r,q)}))\notin\mathcal{E}(4r)}} \sum_{\substack{f_1\mid D(p,q) \\ f_2\mid D(r,q) \\ (f_1f_2,2)=1}} \frac{1}{\varphi(f_1)\varphi(f_2)} \\ & + \left(z\log z + \frac{\log z}{z^{\alpha-1}}\right)\left(\sum_{\substack{p^-<q<p^+ \\ \operatorname{disc}(\mathbb{Q}(\sqrt{D(p,q)}))\in\mathcal{E}(4p) \\ \operatorname{disc}(\mathbb{Q}(\sqrt{D(r,q)}))\notin\mathcal{E}(4r)}} \sum_{\substack{f_1\mid D(p,q) \\ f_2\mid D(r,q) \\ (f_1f_2,2)=1}} \frac{1}{\varphi(f_1)\varphi(f_2)}\right. \\ & \left. + \sum_{\substack{p^-<q<p^+ \\ \operatorname{disc}(\mathbb{Q}(\sqrt{D(p,q)}))\notin\mathcal{E}(4p) \\ \operatorname{disc}(\mathbb{Q}(\sqrt{D(r,q)}))\in\mathcal{E}(4r)}} \sum_{\substack{f_1\mid D(p,q) \\ f_2\mid D(r,q) \\ (f_1f_2,2)=1}} \frac{1}{\varphi(f_1)\varphi(f_2)}\right) \\ & + z^2 \sum_{\substack{p^-<q<p^+ \\ \operatorname{disc}(\mathbb{Q}(\sqrt{D(p,q)}))\in\mathcal{E}(4p) \\ \operatorname{disc}(\mathbb{Q}(\sqrt{D(r,q)}))\in\mathcal{E}(4r)}} \sum_{\substack{f_1\mid D(p,q) \\ f_2\mid D(r,q) \\ (f_1f_2,2)=1}} \frac{1}{\varphi(f_1)\varphi(f_2)}. \end{aligned}$$

For $q \in (p^-, p^+)$ such that $\Delta := \operatorname{disc}(\mathbb{Q}(\sqrt{D(p,q)})) \in \mathcal{E}(4p)$ we have that $D(p,q) = \Delta m^2$ for some $m \in \mathbb{N}$ or, equivalently $(p+1-q)^2 - \Delta m^2 = 4p$. So for each fixed $\Delta \in \mathcal{E}(4p)$, there are at most $\tau(4p) = 6$ admissible values of q. Thus,

$$\#\{p^- < q < p^+ : \operatorname{disc}(\mathbb{Q}(\sqrt{D(p,q)})) \in \mathcal{E}(4p)\} \leq \#\mathcal{E}(4p)\tau(4p) \ll p^{\frac{1}{5}},$$

since $\alpha \geq 10$. Similarly, we have that

$$\#\{p^- < q < p^+ : \operatorname{disc}(\mathbb{Q}(\sqrt{D(r,q)})) \in \mathcal{E}(4r)\} \leq \#\mathcal{E}(4r)\tau(4r) \ll r^{\frac{1}{5}} \ll p^{\frac{1}{5}}$$

and

$$\#\Big\{p^- < q < p^+ : \mathrm{disc}(\mathbb{Q}(\sqrt{D(p,q)})) \in \mathcal{E}(4p) \text{ and } \mathrm{disc}(\mathbb{Q}(\sqrt{D(r,q)})) \in \mathcal{E}(4r)\Big\}$$
$$\leq \min\{\#\mathcal{E}(4p)\tau(4p), \#\mathcal{E}(4r)\tau(4r)\} \ll p^{\frac{1}{5}}.$$

From the bounds of the Euler φ-function in Theorem 2.2.5 and since $f_1 \leq D(p,q)$ we have that

$$\log\log(f_1) \leq \log\log(D(p,q)) \ll \log\log p = \log z.$$

Thus

$$\sum_{\substack{f_1 | D(p,q) \\ (f_1,2)=1}} \frac{1}{\varphi(f_1)} \ll \log z \sum_{\substack{f_1 | D(p,q) \\ (f_1,2)=1}} \frac{1}{f_1} = \log z \prod_{\substack{\ell | D(p,q) \\ \ell \neq 2}} \left(1 - \frac{1}{\ell}\right)^{-1}$$
$$\leq \log z \frac{D(p,q)}{\varphi(D(p,q))} \ll (\log z)^2.$$

The result is analogous for $D(r,q)$ and thus combining the above estimates gives

$$R \ll_\alpha \frac{\sqrt{p}(\log z)^6}{z^{1+\alpha}} + \frac{\sqrt{p}(\log z)^6}{z^{1+2\alpha}} + p^{\frac{1}{5}}(z\log^5 z + z^{1-\alpha}\log^5 z + z^2\log^4 z)$$

and hence the remainder term is smaller than the main term in (4.7) (since $\alpha \geq 10$.)

Now we bound S_2', that is, we show that

$$S_2' := \sum_{p^- < q < p^+} \sum_{\substack{f_1 | D(p,q) \\ f_2 | D(r,q) \\ (f_1 f_2, 2)=1}} \frac{L\left(1, \chi_1; z^{8\alpha^2}\right) L\left(1, \chi_2; z^{8\alpha^2}\right)}{\varphi(f_1)\varphi(f_2)} \ll \frac{\sqrt{p}}{\log p}.$$

First we find an upper bound for $L\left(1, \chi_i; z^{8\alpha^2}\right)$. From Mertens' Theorem, Theorem

2.2.26, we have that

$$\begin{aligned} L(1,\chi_1;z^{8\alpha^2}) &= \prod_{\ell\le\sqrt{z}}\left(1-\frac{\chi_1(\ell)}{\ell}\right)^{-1}\prod_{\sqrt{z}\le\ell\le z^{8\alpha^2}}\left(1-\frac{\chi_1(\ell)}{\ell}\right)^{-1} \\ &\le \prod_{\substack{\ell\le\sqrt{z}\\ \ell\mid 2f_1f_2}}\left(1-\frac{\left(\frac{D(p,q)}{\ell}\right)}{\ell}\right)^{-1}\prod_{\sqrt{z}\le\ell\le z^{8\alpha^2}}\left(1-\frac{1}{\ell}\right)^{-1} \\ &\ll \prod_{\ell\le\sqrt{z}}\left(1-\frac{\left(\frac{D(p,q)}{\ell}\right)}{\ell}\right)^{-1}\prod_{\substack{\ell\le\sqrt{z}\\ \ell\mid 2f_1f_2}}\left(1-\frac{\left(\frac{D(p,q)}{\ell}\right)}{\ell}\right). \end{aligned} \tag{4.8}$$

We consider the two products in (4.8) and find that

$$\begin{aligned} \prod_{\ell\le\sqrt{z}}\left(1-\frac{\left(\frac{D(p,q)}{\ell}\right)}{\ell}\right)^{-1} &= \prod_{\ell\le\sqrt{z}}\left(1+\frac{\left(\frac{D(p,q)}{\ell}\right)}{\ell}\right)\left(1+\sum_{v=1}^{\infty}\left[\frac{\left(\frac{D(p,q)}{\ell}\right)}{\ell}\right]^{2v}\right) \\ &\ll \prod_{\ell\le\sqrt{z}}\left(1+\frac{\left(\frac{D(p,q)}{\ell}\right)}{\ell}\right), \end{aligned} \tag{4.9}$$

and

$$\prod_{\substack{\ell\le\sqrt{z}\\ \ell\mid 2f_1f_2}}\left(1-\frac{\left(\frac{D(p,q)}{\ell}\right)}{\ell}\right)\ll\frac{f_1f_2}{\varphi(f_1)\varphi(f_2)}. \tag{4.10}$$

Combining (4.8), (4.9) and (4.10) gives

$$L(1,\chi_1;z^{8\alpha^2})\ll\frac{f_1f_2}{\varphi(f_1)\varphi(f_2)}\prod_{\ell\le\sqrt{z}}\left(1+\frac{\left(\frac{D(p,q)}{\ell}\right)}{\ell}\right), \tag{4.11}$$

and similarly,

$$L(1,\chi_2;z^{8\alpha^2})\ll\frac{f_1f_2}{\varphi(f_1)\varphi(f_2)}\prod_{\ell\le\sqrt{z}}\left(1+\frac{\left(\frac{D(r,q)}{\ell}\right)}{\ell}\right). \tag{4.12}$$

Now since the products on the RHS of (4.11) and (4.12) no longer depend on f_1 and f_2

we swap the sum and product to obtain the upper bound

$$S_2' \ll \sum_{p^-<q<p^+} \prod_{\ell\le\sqrt{z}} \left(1+\frac{\left(\frac{D(p,q)}{\ell}\right)}{\ell}\right)\left(1+\frac{\left(\frac{D(r,q)}{\ell}\right)}{\ell}\right) \times \sum_{\substack{f_1\mid D(p,q)\\(f_1,2)=1}} \frac{f_1^2}{\varphi^3(f_1)} \sum_{\substack{f_2\mid D(r,q)\\(f_2,2)=1}} \frac{f_2^2}{\varphi^3(f_2)}. \tag{4.13}$$

We need f_1 and f_2 to be coprime and square-free, so we first consider the sum over f_1. Since $\dfrac{f_1^2}{\varphi^3(f_1)}$ is multiplicative we have that

$$\begin{aligned}
\sum_{\substack{f_1\mid D(p,q)\\(f_1,2)=1}} \frac{f_1^2}{\varphi^3(f_1)} &= \prod_{\substack{\ell\mid D(p,q)\\\ell\neq 2}} \left(1+\frac{\ell^3}{(\ell-1)^4}\right)\\
&= \prod_{\substack{\ell\mid D(p,q)\\\ell\neq 2}} \left(1+\frac{1}{\ell}\right)\left(1+\frac{\ell^4-(\ell-1)^4}{(\ell-1)^4(\ell+1)}\right)\\
&\ll \prod_{\substack{\ell\mid D(p,q)\\\ell\nmid 2f_2}} \left(1+\frac{1}{\ell}\right) \prod_{\substack{\ell\mid (D(p,q),f_2)\\\ell\neq 2}} \left(1+\frac{1}{\ell}\right)\\
&\le \prod_{\substack{\ell\mid D(p,q)\\\ell\nmid 2f_2}} \left(1+\frac{1}{\ell}\right) \prod_{\substack{\ell\mid (D(p,q),f_2)\\\ell\neq 2}} \left(1-\frac{1}{\ell}\right)^{-1}\\
&\ll \frac{f_2}{\varphi(f_2)} \prod_{\substack{\ell\mid D(p,q)\\\ell\nmid 2f_2}} \left(1+\frac{1}{\ell}\right)\\
&= \frac{f_2}{\varphi(f_2)} \prod_{\substack{\ell\mid D(p,q)\\\ell\nmid 2f_2\\\ell\le z^{\alpha}}} \left(1+\frac{1}{\ell}\right)\left(1+O(z^{-\alpha+1})\right)\\
&\ll \frac{f_2}{\varphi(f_2)} \prod_{\substack{\ell\mid D(p,q)\\\ell\nmid 2f_2\\\ell\le\sqrt{z}}} \left(1+\frac{1}{\ell}\right) = \frac{f_2}{\varphi(f_2)} \sum_{\substack{f_1\mid D(p,q)\\(f_1,2f_2)=1\\P^+(f_1)\le\sqrt{z}}} \frac{\mu^2(f_1)}{f_1},
\end{aligned} \tag{4.14}$$

by Mertens' Theorem, Theorem 2.2.26 and similarly,

$$\sum_{\substack{f_2|D(r,q)\\(f_2,2f_1)=1}} \frac{f_2^3}{\varphi^4(f_2)} = \prod_{\substack{\ell|D(r,q)\\(\ell,2f_1)=1}} \left(1+\frac{\ell^4}{(\ell-1)^5}\right) \ll \sum_{\substack{f_2|D(r,q)\\(f_2,2f_1)=1\\P^+(f_2)\leq\sqrt{z}}} \frac{\mu^2(f_2)}{f_2}. \tag{4.15}$$

Combining (4.13), (4.14) and (4.15) we have that

$$\begin{aligned} S_2' \ll & \sum_{p^-<q<p^+} \prod_{\ell\leq\sqrt{z}} \left(1+\frac{\left(\frac{D(p,q)}{\ell}\right)}{\ell}\right)\left(1+\frac{\left(\frac{D(r,q)}{\ell}\right)}{\ell}\right) \\ & \times \sum_{\substack{f_1|D(p,q)\\(f_1,2)=1\\P^+(f_1)\leq\sqrt{z}}} \frac{\mu^2(f_1)}{f_1} \sum_{\substack{f_2|D(r,q)\\(f_2,2f_1)=1\\P^+(f_2)\leq\sqrt{z}}} \frac{\mu^2(f_2)}{f_2}. \end{aligned} \tag{4.16}$$

Now we require that f_1 and f_2 are coprime in the product in (4.16). From (4.10) we have that

$$\begin{aligned} \prod_{\ell\leq\sqrt{z}} \left(1+\frac{\left(\frac{D(p,q)}{\ell}\right)}{\ell}\right) &= \prod_{\substack{\ell\leq\sqrt{z}\\\ell\nmid 2f_1f_2}} \left(1+\frac{\left(\frac{D(p,q)}{\ell}\right)}{\ell}\right) \prod_{\substack{\ell\leq\sqrt{z}\\\ell|2f_1f_2}} \left(1+\frac{\left(\frac{D(p,q)}{\ell}\right)}{\ell}\right) \\ &\ll \frac{f_1f_2}{\varphi(f_1)\varphi(f_2)} \prod_{\substack{\ell\leq\sqrt{z}\\\ell\nmid 2f_1f_2}} \left(1+\frac{\left(\frac{D(p,q)}{\ell}\right)}{\ell}\right), \end{aligned} \tag{4.17}$$

and similarly,

$$\prod_{\ell\leq\sqrt{z}} \left(1+\frac{\left(\frac{D(r,q)}{\ell}\right)}{\ell}\right) \ll \frac{f_1f_2}{\varphi(f_1)\varphi(f_2)} \prod_{\substack{\ell\leq\sqrt{z}\\\ell\nmid 2f_1f_2}} \left(1+\frac{\left(\frac{D(r,q)}{\ell}\right)}{\ell}\right). \tag{4.18}$$

Combining (4.16), (4.17) and (4.18) gives

$$S_2' \ll \sum_{p^-<q<p^+} \sum_{\substack{f_1 \mid D(p,q) \\ (f_1,2)=1 \\ P^+(f_1)\le\sqrt{z}}} \frac{\mu^2(f_1)f_1}{\varphi^2(f_1)} \sum_{\substack{f_2 \mid D(r,q) \\ (f_2,2f_1)=1 \\ P^+(f_2)\le\sqrt{z}}} \frac{\mu^2(f_2)f_2}{\varphi^2(f_2)}$$
$$\times \prod_{\substack{\ell\le\sqrt{z} \\ \ell\nmid 2f_1f_2}} \left(1+\frac{\left(\frac{D(p,q)}{\ell}\right)}{\ell}\right)\left(1+\frac{\left(\frac{D(r,q)}{\ell}\right)}{\ell}\right)$$
$$= \sum_{\substack{P^+(f_1),P^+(f_2)\le\sqrt{z} \\ (f_1,2)=(f_2,2f_1)=1}} \frac{\mu^2(f_1)\mu^2(f_2)f_1f_2}{\varphi^2(f_1)\varphi^2(f_2)} \sum_{\substack{p^-<q<p^+ \\ f_1\mid D(p,q) \\ f_2\mid D(r,q)}} \prod_{\substack{\ell\le\sqrt{z} \\ \ell\nmid 2f_1f_2}} \left(1+\frac{\left(\frac{D(p,q)}{\ell}\right)}{\ell}\right)\left(1+\frac{\left(\frac{D(r,q)}{\ell}\right)}{\ell}\right). \tag{4.19}$$

We have that

$$\prod_{\substack{\ell\le\sqrt{z} \\ \ell\nmid 2f_1f_2}} \left(1+\frac{\left(\frac{D(p,q)}{\ell}\right)}{\ell}\right) = \sum_{\substack{P^+(n_1)\le\sqrt{z} \\ (n_1,2f_1f_2)=1}} \frac{\mu^2(n_1)}{n_1}\left(\frac{D(p,q)}{n_1}\right), \tag{4.20}$$

and likewise we have that

$$\prod_{\substack{\ell\le\sqrt{z} \\ \ell\nmid 2f_1f_2}} \left(1+\frac{\left(\frac{D(r,q)}{\ell}\right)}{\ell}\right) = \sum_{\substack{P^+(n_2)\le\sqrt{z} \\ (n_2,2f_1f_2)=1}} \frac{\mu^2(n_2)}{n_2}\left(\frac{D(r,q)}{n_2}\right). \tag{4.21}$$

We require q coprime to $2f_1f_2n_1n_2$ so we have that the RHS of (4.19) becomes

$$\begin{aligned}
&\sum_{\substack{P^+(f_1),P^+(f_2)\le\sqrt{z}\\(f_1,2)=(f_2,2f_1)=1}}\frac{\mu^2(f_1)\mu^2(f_2)f_1f_2}{\varphi^2(f_1)\varphi^2(f_2)}\sum_{\substack{P^+(n_1),P^+(n_2)\le\sqrt{z}\\(n_1n_2,2f_1f_2)=1}}\frac{\mu^2(n_1)\mu^2(n_2)}{n_1n_2}\\
&\times\sum_{\substack{p^-<q<p^+\\f_1|D(p,q)\\f_2|D(r,q)\\(q,2f_1f_2n_1n_2)=1}}\left(\frac{D(p,q)}{n_1}\right)\left(\frac{D(r,q)}{n_2}\right)\\
&+\sum_{\substack{P^+(f_1),P^+(f_2)\le\sqrt{z}\\(f_1,2)=(f_2,2f_1)=1}}\frac{\mu^2(f_1)\mu^2(f_2)f_1f_2}{\varphi^2(f_1)\varphi^2(f_2)}\sum_{\substack{P^+(n_1),P^+(n_2)\le\sqrt{z}\\(n_1n_2,2f_1f_2)=1}}\frac{\mu^2(n_1)\mu^2(n_2)}{n_1n_2}\\
&\times\sum_{\substack{p^-<q<p^+\\f_1|D(p,q)\\f_2|D(r,q)\\q|2f_1f_2n_1n_2}}\left(\frac{D(p,q)}{n_1}\right)\left(\frac{D(r,q)}{n_2}\right)
\end{aligned}\tag{4.22}$$

We have that the second sum in (4.22) is bounded by

$$\ll\sum_{\substack{P^+(f_1),P^+(f_2)\le\sqrt{z}\\(f_1,2)=(f_2,2f_1)=1}}\frac{\mu^2(f_1)\mu^2(f_2)f_1f_2\tau(f_1)\tau(f_2)}{\varphi^2(f_1)\varphi^2(f_2)}\sum_{\substack{P^+(n_1),P^+(n_2)\le\sqrt{z}\\(n_1n_2,2f_1f_2)=1}}\frac{\mu^2(n_1)\mu^2(n_2)\tau(n_1n_2)}{n_1n_2}.\tag{4.23}$$

Then for some $\epsilon>0$ the inner sum in (4.23) becomes

$$\sum_{\substack{P^+(n_1),P^+(n_2)\le\sqrt{z}\\(n_1n_2,2f_1f_2)=1}}\frac{\mu^2(n_1)\mu^2(n_2)\tau(n_1n_2)}{n_1n_2}\ll\sum_{\substack{P^+(n_1)\le\sqrt{z}\\(n_1,2f_1f_2)=1}}n_1^{\epsilon-1}\sum_{\substack{P^+(n_2)\le\sqrt{z}\\(n_2,2f_1f_2)=1}}n_2^{\epsilon-1}\ll z^{\epsilon}\log^2 z$$

by partial summation and for $i=1,2$ we have that

$$\sum_{\substack{P^+(f_i)\le\sqrt{z}\\(f_i,2)=1}}\frac{\mu^2(f_i)f_i\tau(f_i)}{\varphi^2(f_i)}\ll\sum_{\substack{P^+(f_i)\le\sqrt{z}\\(f_i,2)=1}}\frac{(\log\log f_i)^2}{f_i^{1-\epsilon}}\ll z^{\epsilon}\log z(\log\log z)^2.$$

Hence, the second term in (4.22) is smaller than the main term and we have that

$$S_2' \ll \sum_{\substack{P^+(f_1),P^+(f_2)\le\sqrt{z}\\(f_1,2)=(f_2,2f_1)=1}} \frac{\mu^2(f_1)\mu^2(f_2)f_1f_2}{\varphi^2(f_1)\varphi^2(f_2)} \sum_{\substack{P^+(n_1),P^+(n_2)\le\sqrt{z}\\(n_1n_2,2f_1f_2)=1}} \frac{\mu^2(n_1)\mu^2(n_2)}{n_1n_2}$$
$$\times \sum_{\substack{p^-<q<p^+\\f_1|D(p,q)\\f_2|D(r,q)\\(q,2f_1f_2n_1n_2)=1}} \left(\frac{D(p,q)}{n_1}\right)\left(\frac{D(r,q)}{n_2}\right) \tag{4.24}$$

We will now use the fundamental lemma for the combinatorial sieve, Lemma 2.2.28 with $y = p^{\frac{1}{4}}$ and $D = y^2$ to bound the innermost sum of (4.19). So we extend the summation from primes q to integers m with no prime factors $\le y$.

Consequently, we have that (4.24) is less than or equal to the same sum with a weight, that is,

$$S_2' \ll \sum_{\substack{P^+(f_1),P^+(f_2)\le\sqrt{z}\\(f_1,2)=(f_2,2f_1)=1}} \frac{\mu^2(f_1)\mu^2(f_2)f_1f_2}{\varphi^2(f_1)\varphi^2(f_2)} \sum_{\substack{P^+(n_1),P^+(n_2)\le\sqrt{z}\\(n_1n_2,2f_1f_2)=1}} \frac{\mu^2(n_1)\mu^2(n_2)}{n_1n_2}$$
$$\times \sum_{\substack{p^-<q<p^+\\f_1|D(p,q)\\f_2|D(r,q)\\(q,2f_1f_2n_1n_2)=1}} \left(\frac{D(p,q)}{n_1}\right)\left(\frac{D(r,q)}{n_2}\right)$$
$$\le \sum_{\substack{P^+(f_1),P^+(f_2)\le\sqrt{z}\\(f_1,2)=(f_2,2f_1)=1}} \frac{\mu^2(f_1)\mu^2(f_2)f_1f_2}{\varphi^2(f_1)\varphi^2(f_2)} \sum_{\substack{P^+(n_1),P^+(n_2)\le\sqrt{z}\\(n_1n_2,2f_1f_2)=1}} \frac{\mu^2(n_1)\mu^2(n_2)}{n_1n_2}$$
$$\times \sum_{\substack{p^-\le m\le p^+\\f_1|D(p,m)\\f_2|D(r,m)\\(m,2f_1f_2n_1n_2)=1}} (\lambda^+ * 1)(m)\left(\frac{D(p,m)}{n_1}\right)\left(\frac{D(r,m)}{n_2}\right) := S_3, \tag{4.25}$$

by the positivity of the Euler product in (4.20) and (4.21).

Then we have that the RHS of (4.25) becomes

$$S_3 = \sum_{\substack{P^+(f_1),P^+(f_2)\le\sqrt{z}\\(f_1,2)=(f_2,2f_1)=1}} \frac{\mu^2(f_1)\mu^2(f_2)f_1f_2}{\varphi^2(f_1)\varphi^2(f_2)} \sum_{\substack{P^+(n_1),P^+(n_2)\le\sqrt{z}\\(n_1n_2,2f_1f_2)=1}} \frac{\mu^2(n_1)\mu^2(n_2)}{n_1n_2}$$
$$\times \sum_{\substack{a\le D\\(a,2f_1f_2n_1n_2)=1}} \lambda^+(a) \sum_{\substack{p^-<m<p^+\\f_1|D(p,m)\\f_2|D(r,m)\\a|m}} \left(\frac{D(p,m)}{n_1}\right)\left(\frac{D(r,m)}{n_2}\right), \tag{4.26}$$

since λ^+ is supported on integers, $a \mid m, a \le D, (m, 2f_1f_2n_1n_2) = 1$.

Now we will split the integers in the interval $m \in (p^-, p^+)$ according to the congruence class of $D(p,m) \pmod{n_1}$ and $D(r,m) \pmod{n_2}$ and we have that (4.26) becomes

$$S_3 = \sum_{\substack{P^+(f_1),P^+(f_2)\le\sqrt{z}\\(f_1,2)=(f_2,2f_1)=1}} \frac{\mu^2(f_1)\mu^2(f_2)f_1f_2}{\varphi^2(f_1)\varphi^2(f_2)} \sum_{\substack{P^+(n_1),P^+(n_2)\le\sqrt{z}\\(n_1n_2,2f_1f_2)=1}} \frac{\mu^2(n_1)\mu^2(n_2)}{n_1n_2}$$
$$\times \sum_{\substack{a\le D\\(a,2f_1f_2n_1n_2)=1}} \lambda^+(a) \sum_{\substack{b_1\in\mathbb{Z}/n_1\mathbb{Z}\\b_2\in\mathbb{Z}/n_2\mathbb{Z}}} \left(\frac{b_1}{n_1}\right)\left(\frac{b_2}{n_2}\right) S(a,f_1,f_2,n_1,n_2,b_1,b_2),$$

where we define

$$S(a,f_1,f_2,n_1,n_2,b_1,b_2) := \#\left\{\begin{array}{ll} p^- < m < p^+ & m \equiv 0 \pmod{a} \\ D(p,m) \equiv 0 \pmod{f_1} & D(r,m) \equiv 0 \pmod{f_2} \\ D(p,m) \equiv b_1 \pmod{n_1} & D(r,m) \equiv b_2 \pmod{n_2} \end{array}\right\}.$$

Let $\Delta_1(m) := D(p,m), \Delta_2(m) := D(r,m)$. Then we have that

$$S(a,f_1,f_2,n_1,n_2,b_1,b_2) = \left(\frac{4\sqrt{p}}{af_1f_2[n_1,n_2]}\right) \#T(a,f_1,f_2,n_1,n_2,b_1,b_2)$$
$$+ O(\#T(a,f_1,f_2,n_1,n_2,b_1,b_2)), \tag{4.27}$$

where

$$T(a,f_1,f_2,n_1,n_2,b_1,b_2) := \left\{ m \in \mathbb{Z}/af_1f_2[n_1,n_2]\mathbb{Z} : \begin{array}{l} \Delta_1(m) \equiv 0 \pmod{f_1} \\ \Delta_2(m) \equiv 0 \pmod{f_2} \\ \Delta_1(m) \equiv b_1 \pmod{n_1} \\ \Delta_2(m) \equiv b_2 \pmod{n_2} \\ m \equiv 0 \pmod{a} \end{array} \right\},$$

since $a, f_1, f_2, [n_1, n_2]$ are all coprime. Therefore, we have from (4.27) that (4.26) becomes

$$\begin{aligned} S_3 =& 4\sqrt{p} \sum_{\substack{P^+(f_1),P^+(f_2)\le\sqrt{z} \\ (f_1,2)=(f_2,2f_1)=1}} \frac{\mu^2(f_1)\mu^2(f_2)}{\varphi^2(f_1)\varphi^2(f_2)} \sum_{\substack{P^+(n_1),P^+(n_2)\le\sqrt{z} \\ (n_1n_2,2f_1f_2)=1}} \frac{\mu^2(n_1)\mu^2(n_2)}{n_1n_2[n_1,n_2]} \\ &\times \sum_{\substack{a\le D \\ (a,2f_1f_2n_1n_2)=1}} \frac{\lambda^+(a)}{a} \sum_{\substack{b_1\in\mathbb{Z}/n_1\mathbb{Z} \\ b_2\in\mathbb{Z}/n_2\mathbb{Z}}} \left(\frac{b_1}{n_1}\right)\left(\frac{b_2}{n_2}\right) \#T(a,f_1,f_2,n_1,n_2,b_1,b_2) \\ &+ O\Bigg(\sum_{\substack{P^+(f_1),P^+(f_2)\le\sqrt{z} \\ (f_1,2)=(f_2,2f_1)=1}} \frac{\mu^2(f_1)\mu^2(f_2)f_1f_2}{\varphi^2(f_1)\varphi^2(f_2)} \sum_{\substack{P^+(n_1),P^+(n_2)\le\sqrt{z} \\ (n_1n_2,2f_1f_2)=1}} \frac{\mu^2(n_1)\mu^2(n_2)}{n_1n_2} \\ &\times \sum_{\substack{a\le D \\ (a,2f_1f_2n_1n_2)=1}} |\lambda^+(a)| \sum_{\substack{b_1\in\mathbb{Z}/n_1\mathbb{Z} \\ b_2\in\mathbb{Z}/n_2\mathbb{Z}}} \#T(a,f_1,f_2,n_1,n_2,b_1,b_2) \Bigg). \end{aligned} \tag{4.28}$$

Since both sums in (4.28) are over square-free numbers, by the Chinese remainder theorem we have that

$$\#T(a,f_1,f_2,n_1,n_2,b_1,b_2) = h_1(f_1,0)h_2(f_2,0) \prod_{\ell\mid[n_1,n_2]} \#T^{(\ell)}(n_1,n_2,b_1,b_2)$$

where we define

$$h_i(u,v) := \#\{m \in \mathbb{Z}/u\mathbb{Z} : \Delta_i(m) \equiv v \pmod{u}\}, \tag{4.29}$$

and

$$T^{(\ell)}(n_1,n_2,b_1,b_2) := \Big\{ m \in \mathbb{Z}/\ell^{\nu_\ell([n_1,n_2])}\mathbb{Z} : \Delta_1(m) \equiv b_1 \pmod{\ell^{\nu_\ell(n_1)}} \\ \text{and } \Delta_2(m) \equiv b_2 \pmod{\ell^{\nu_\ell(n_2)}} \Big\}. \tag{4.30}$$

Note that $h_i(u,v)$ is multiplicative in u and if u is square-free then we have that

$$\begin{aligned} h_i(u,v) &= \prod_{\ell|u} \#\{m \in \mathbb{Z}/\ell\mathbb{Z} : (p+1-m)^2 \equiv 4p+v \pmod{\ell}\} \\ &= \prod_{\ell|u} \left(1 + \left(\frac{4p+v}{\ell}\right)\right). \end{aligned} \tag{4.31}$$

Thus, $|h_i(u,v)| \le \tau(u)$ for all square-free integers u. Now define

$$c(n_1,n_2) := \sum_{\substack{b_1 \in \mathbb{Z}/n_1\mathbb{Z} \\ b_2 \in \mathbb{Z}/n_2\mathbb{Z}}} \left(\frac{b_1}{n_1}\right)\left(\frac{b_2}{n_2}\right) \prod_{\ell|[n_1,n_2]} \#T^{(\ell)}(n_1,n_2,b_1,b_2).$$

We have that $c(n_1,n_2)$ is multiplicative in n_1 and n_2, that is if $n_1 = n_1'n_1'', n_2 = n_2'n_2''$ and $(n_1'n_2', n_1''n_2'') = 1$ then $c(n_1,n_2) = c(n_1',n_2')c(n_1'',n_2'')$. If $(n_1'n_2', n_1''n_2'') = 1$ then $[n_1'n_1'', n_2'n_2''] = [n_1',n_2'][n_1'',n_2'']$ and we have by the Chinese remainder theorem that

$$\begin{aligned} c(n_1'n_1'', n_2'n_2'') &= \sum_{\substack{b_1 \in \mathbb{Z}/n_1'n_1''\mathbb{Z} \\ b_2 \in \mathbb{Z}/n_2'n_2''\mathbb{Z}}} \left(\frac{b_1}{n_1'n_1''}\right)\left(\frac{b_2}{n_2'n_2''}\right) \prod_{\ell|[n_1'n_1'', n_2'n_2'']} \#T^{(\ell)}(n_1'n_1'', n_2'n_2'', b_1, b_2) \\ &= \sum_{\substack{b_1' \in \mathbb{Z}/n_1'\mathbb{Z} \\ b_2' \in \mathbb{Z}/n_2'\mathbb{Z}}} \left(\frac{b_1'}{n_1'}\right)\left(\frac{b_2'}{n_2'}\right) \prod_{\ell|[n_1',n_2']} \#T^{(\ell)}(n_1',n_2',b_1',b_2') \\ &\times \sum_{\substack{b_1'' \in \mathbb{Z}/n_1''\mathbb{Z} \\ b_2'' \in \mathbb{Z}/n_2''\mathbb{Z}}} \left(\frac{b_1''}{n_1''}\right)\left(\frac{b_2''}{n_2''}\right) \prod_{\ell|[n_1'',n_2'']} \#T^{(\ell)}(n_1'',n_2'',b_1'',b_2'') \\ &= c(n_1',n_2')c(n_1'',n_2''). \end{aligned}$$

Since n_1, n_2 runs over square-free integers with $(n_1n_2, 2f_1f_2) = 1$ it is enough to

calculate $c(n_1, n_2)$ for primes $\ell \nmid 2f_1f_2$ and we have three cases to consider, since $c(1,1) = 1$, namely, $c(\ell, 1), c(1, \ell)$ and $c(\ell, \ell)$.

The cases $c(\ell, 1)$ and $c(1, \ell)$ are completely similar and we have from (4.30) and (4.31) that

$$\begin{aligned} c(\ell,1) &= \sum_{b_1 \in \mathbb{Z}/\ell\mathbb{Z}} \left(\frac{b_1}{\ell}\right) h_1(\ell, b_1) \\ &= \sum_{b_1 \in \mathbb{Z}/\ell\mathbb{Z}} \left(\frac{b_1}{\ell}\right) \left(1 + \left(\frac{4p+b_1}{\ell}\right)\right) = \sum_{b_1 \in \mathbb{Z}/\ell\mathbb{Z}} \left(\frac{b_1}{\ell}\right) \left(\frac{4p+b_1}{\ell}\right) \\ &= \sum_{b_1 \in \mathbb{Z}/\ell\mathbb{Z}} \left(\frac{b_1^2 + 4pb_1}{\ell}\right) = c(1,\ell). \end{aligned}$$

From [Ste, Exercise 1.1.9] we have for $a \not\equiv 0 \pmod{\ell}$ that

$$\sum_{t \pmod{\ell}} \left(\frac{at^2+bt+c}{\ell}\right) = \begin{cases} \left(\frac{a}{\ell}\right)(\ell-1) & \text{if } b^2 - 4ac \equiv 0 \pmod{\ell}, \\ -\left(\frac{a}{\ell}\right) & \text{if } b^2 - 4ac \not\equiv 0 \pmod{\ell}. \end{cases}$$

Thus,

$$c(\ell,1) = \begin{cases} \ell - 1 & \text{if } 16p^2 \equiv 0 \pmod{\ell}, \\ -1 & \text{if } 16p^2 \not\equiv 0 \pmod{\ell}. \end{cases}$$

However, $\ell \nmid 2$ so if $16p^2 \equiv 0 \pmod{\ell}$ then $\ell = p$. Since $P^+(n_1) \leq \sqrt{z} = \sqrt{\log p} < p$, we have that $c(\ell, 1) = c(1, \ell) = -1$.

In the $c(\ell, \ell)$ case we have that

$$c(\ell,\ell) := \sum_{b_1, b_2 \in \mathbb{Z}/\ell\mathbb{Z}} \left(\frac{b_1 b_2}{\ell}\right) \#T^{(\ell)}(\ell, \ell, b_1, b_2),$$

where

$$T^{(\ell)}(\ell,\ell,b_1,b_2) = \{m \in \mathbb{Z}/\ell\mathbb{Z} : \Delta_1(m) \equiv b_1 \pmod{\ell} \text{ and } \Delta_2(m) \equiv b_2 \pmod{\ell}\}.$$

We remark that there are at most two solutions to the equation $\Delta_1(m) \equiv b_1 \pmod{\ell}$

since $\Delta_1(m)$ is a quadratic polynomial in m. Let m_0 be one such solution. If $\Delta_2(m_0) \not\equiv b_2 \pmod{\ell}$ then the two equations are not compatible. If $\Delta_2(m_0) \equiv b_2 \pmod{\ell}$ then since the trace of $\Delta_2(m)$ is fixed there will be at most 2 values of b_2 that satisfy this equation. Hence,

$$|c(\ell,\ell)| \leq \sum_{b_1 \in \mathbb{Z}/\ell\mathbb{Z}} 2 = 2\ell.$$

Combining the three cases, we conclude

$$|c(n_1,n_2)| \leq \prod_{\ell|(n_1,n_2)} |c(\ell,\ell)| \leq \prod_{\ell|(n_1,n_2)} 2\ell = 2^{\omega((n_1,n_2))}(n_1,n_2).$$

We now place our bounds for $h_i(f_i,0)$ and $c(n_1,n_2)$ into (4.28) and we have that

$$\begin{aligned} S_3 \ll & \sqrt{p} \sum_{\substack{P^+(f_1),P^+(f_2)\leq\sqrt{z}\\(f_1,2)=(f_2,2f_1)=1}} \frac{\mu^2(f_1)\mu^2(f_2)\tau(f_1)\tau(f_2)}{\varphi^2(f_1)\varphi^2(f_2)} \sum_{\substack{P^+(n_1),P^+(n_2)\leq\sqrt{z}\\(n_1n_2,2f_1f_2)=1}} \frac{\mu^2(n_1)\mu^2(n_2)(n_1,n_2)^2}{(n_1n_2)^{2-\epsilon}} \\ & \times \left| \sum_{\substack{a\leq D\\(a,2f_1f_2n_1n_2)=1}} \frac{\lambda^+(a)}{a} \right| + D \sum_{\substack{P^+(f_1),P^+(f_2)\leq\sqrt{z}\\(f_1,2)=(f_2,2f_1)=1}} \frac{\mu^2(f_1)\mu^2(f_2)f_1f_2\tau(f_1)\tau(f_2)}{\varphi^2(f_1)\varphi^2(f_2)} \\ & \times \sum_{\substack{P^+(n_1),P^+(n_2)\leq\sqrt{z}\\(n_1n_2,2f_1f_2)=1}} \frac{\mu^2(n_1)\mu^2(n_2)}{n_1n_2} \sum_{\substack{b_1\in\mathbb{Z}/n_1\mathbb{Z}\\b_2\in\mathbb{Z}/n_2\mathbb{Z}}} \prod_{\ell|[n_1,n_2]} \#T^{(\ell)}(n_1,n_2,b_1,b_2). \end{aligned} \tag{4.32}$$

We first consider the second sum in (4.32). Similarly to the function $c(n_1,n_2)$ defined above, we define the function

$$k(n_1,n_2) := \sum_{\substack{b_1\in\mathbb{Z}/n_1\mathbb{Z}\\b_2\in\mathbb{Z}/n_2\mathbb{Z}}} \prod_{\ell|[n_1,n_2]} \#T^{(\ell)}(n_1,n_2,b_1,b_2),$$

which is also multiplicative in n_1 and n_2. We have $k(1,1)=1$,

$$k(\ell,1) = \sum_{b_1\in\mathbb{Z}/\ell\mathbb{Z}} \left(1+\left(\frac{4p+b_1}{\ell}\right)\right) = \ell = k(1,\ell)$$

and as in the case $c(\ell,\ell)$ above, we have that $|k(\ell,\ell)| \leq \sum_{b_1 \in \mathbb{Z}/\ell\mathbb{Z}} 2 = 2\ell$. Thus,

$$|k(n_1,n_2)| \leq \prod_{\ell | [n_1,n_2]} |k(\ell,1)k(1,\ell)k(\ell,\ell)| \leq \prod_{\ell | [n_1,n_2]} 2\ell^3 = 2^{\omega([n_1,n_2])}[n_1,n_2]^3.$$

By Mertens' Theorem, Theorem 2.2.26 and Theorem 2.2.6 for $i = 1, 2$ we have that

$$\sum_{\substack{P^+(f_i) \leq \sqrt{z} \\ (f_i,2)=1}} \frac{\mu^2(f_i)\tau(f_i)f_i}{\varphi^2(f_i)} \ll \frac{\sqrt{z}}{\log z} \prod_{p \leq \sqrt{z}} \left(1 + \frac{2}{(p-1)^2}\right) \ll \frac{\sqrt{z}}{\log z}$$

and we have that

$$\sum_{\substack{P^+(n_1),P^+(n_2) \leq \sqrt{z} \\ (n_1n_2,2f_1f_2)=1}} \frac{\mu^2(n_1)\mu^2(n_2)}{n_1n_2} 2^{\omega([n_1,n_2])}[n_1,n_2]^3 \ll z^{3+\epsilon},$$

for some $\epsilon > 0$ and hence, the second term in (4.32) is $\ll Dz^{4+\epsilon}$. Then from Lemma 2.2.28 we have that (4.32) becomes

$$\begin{aligned} S_3 \ll & \sqrt{p} \sum_{\substack{P^+(f_1),P^+(f_2) \leq \sqrt{z} \\ (f_1,2)=(f_2,2f_1)=1}} \frac{\mu^2(f_1)\mu^2(f_2)\tau(f_1)\tau(f_2)}{\varphi^2(f_1)\varphi^2(f_2)} \sum_{\substack{P^+(n_1),P^+(n_2) \leq \sqrt{z} \\ (n_1n_2,2f_1f_2)=1}} \frac{\mu^2(n_1)\mu^2(n_2)(n_1,n_2)^2}{n_1^{2-\epsilon}n_2^{2-\epsilon}} \\ & \times \prod_{\substack{\ell \leq y \\ \ell \nmid 2f_1f_2n_1n_2}} \left(1 - \frac{1}{\ell}\right) + Dz^{4+\epsilon}. \end{aligned} \tag{4.33}$$

By Mertens' Theorem, Theorem 2.2.26 we have that

$$\prod_{\substack{\ell \leq y \\ \ell \nmid 2f_1f_2n_1n_2}} \left(1 - \frac{1}{\ell}\right) \ll \frac{f_1f_2n_1n_2}{\varphi(f_1)\varphi(f_2)\varphi(n_1)\varphi(n_2)\log y},$$

which gives that (4.33) becomes

$$S_3 \ll \frac{\sqrt{p}}{\log(y)} \sum_{\substack{P^+(f_1),P^+(f_2)\leq\sqrt{z}\\(f_1,2)=(f_2,2f_1)=1}} \frac{\mu^2(f_1)\mu^2(f_2)\tau(f_1)\tau(f_2)f_1f_2}{\varphi^3(f_1)\varphi^3(f_2)}$$
$$\times \sum_{\substack{P^+(n_1),P^+(n_2)\leq\sqrt{z}\\(n_1n_2,2f_1f_2)=1}} \frac{\mu^2(n_1)\mu^2(n_2)(n_1,n_2)^2}{\varphi(n_1)\varphi(n_2)(n_1n_2)^{1-\epsilon}} + Dz^{4+\epsilon}.$$

We have that

$$\sum_{\substack{P^+(n_1),P^+(n_2)\leq\sqrt{z}\\(n_1n_2,2f_1f_2)=1}} \frac{\mu^2(n_1)\mu^2(n_2)(n_1,n_2)^2}{\varphi(n_1)\varphi(n_2)(n_1n_2)^{1-\epsilon}}$$
$$\ll \sum_{\substack{P^+(d)\leq\sqrt{z}\\(d,2f_1f_2)=1}} \frac{\mu^2(d)}{d^{2-2\epsilon}} \sum_{\substack{P^+(m_1),P^+(m_2)\leq\frac{\sqrt{z}}{d}\\n_1=dm_1,n_2=dm_2\\(d,m_1m_2)=1\\(m_1m_2,2f_1f_2)=1}} \frac{\mu^2(m_1)\mu^2(m_2)(\log\log dm_1)(\log\log dm_2)}{(m_1m_2)^{2-\epsilon}} \ll 1,$$

and

$$\sum_{\substack{P^+(f_1),P^+(f_2)\leq\sqrt{z}\\(f_1,2)=(f_2,2f_1)=1}} \frac{\mu^2(f_1)\mu^2(f_2)\tau(f_1)\tau(f_2)f_1f_2}{\varphi^3(f_1)\varphi^3(f_2)}$$
$$\ll \sum_{\substack{P^+(f_1)\leq\sqrt{z}\\(f_1,2)=1}} \frac{\mu^2(f_1)\tau(f_1)(\log\log f_1)^3}{f_1^2} \sum_{\substack{P^+(f_2)\leq\sqrt{z}\\(f_2,2f_1)=1}} \frac{\mu^2(f_2)\tau(f_2)(\log\log f_2)^3}{f_2^2} \ll 1.$$

Thus, we conclude that

$$S_2 \ll S_2' \ll S_3 \ll \frac{\sqrt{p}}{\log y} + D(\log p)^{4+\epsilon} \ll \frac{\sqrt{p}}{\log p},$$

for $y = p^{\frac{1}{6}}, D = (p^{\frac{1}{6}})^2 = p^{\frac{1}{3}}$, which completes the proof. □

We now give an upper bound for the sum in (4.2).

Proposition 4.1.3. *Let p, q be distinct primes in the range $p^- < q < p^+$. Then we have*

that

$$\sum_{p^-<q<p^+} H(D(p,q)) \ll \frac{p}{\log(p)}. \tag{4.34}$$

Proof. The proof of Proposition 4.1.3 follows analogously to the steps taken in Proposition 4.1.2 and is essentially a special case of Chandee, David, Koukoulopoulos and Smith [CDKS, Proposition 4.1]. From the analytic class number formula we have that

$$\sum_{\substack{p^-<q<p^+ \\ q \text{ prime}}} H(D(p,q)) = \sum_{p^-<q<p^+} \sum_{\substack{f^2 \mid D(p,q) \\ (f,2)=1}} \frac{\sqrt{D(p,q)}}{2\pi f} L\left(1, \left(\frac{D(p,q)/f^2}{\cdot}\right)\right).$$

With the goal of obtaining an upper bound, we define as before

$$S_1 := \sum_{p^-<q<p^+} \sum_{\substack{f^2 \mid D(p,q) \\ (f,2)=1}} L\left(1, \left(\frac{D(p,q)/f^2}{\cdot}\right)\right) \frac{1}{f}. \tag{4.35}$$

Analogously to the bound in (4.5), if ℓ is a prime dividing f, then $\ell \mid D(p,q)$ and we have that

$$\begin{aligned} L\left(1, \left(\frac{D(p,q)/f^2}{\cdot}\right)\right) &= \prod_{\ell} \left(1 - \left(\frac{D(p,q)/f^2}{\ell}\right)\frac{1}{\ell}\right)^{-1} \\ &\leq \frac{2f}{\varphi(f)} L\left(1, \left(\frac{(2f)^2 D(p,q)}{\cdot}\right)\right). \end{aligned}$$

To ease notation we define $\chi := \left(\frac{(2f)^2 D(p,q)}{\cdot}\right)$ and thus

$$S_1 \ll \sum_{p^-<q<p^+} \sum_{\substack{f^2 \mid D(p,q) \\ (f,2)=1}} \frac{L(1,\chi)}{\varphi(f)} \leq \sum_{p^-<q<p^+} \sum_{\substack{f \mid D(p,q) \\ (f,2)=1}} \frac{L(1,\chi)}{\varphi(f)}, \tag{4.36}$$

since the sum on the RHS in (4.36) is longer than the sum in (4.35). Since

$$\sum_{p^-<q<p^+} H(D(p,q)) \ll \sqrt{p} S_1,$$

we have as in the previous case the remainder of the proof is reduced to showing the following upper bound

$$S_2 := \sum_{p^- < q < p^+} \sum_{\substack{f \mid D(p,q) \\ (f,2)=1}} \frac{L(1,\chi)}{\varphi(f)} \ll \frac{\sqrt{p}}{\log p}. \tag{4.37}$$

Now let S_2' denote the same sum on the LHS of (4.37) but with $L\left(1,\chi; z^{8\alpha^2}\right)$ in place of $L(1,\chi)$, where we define $z := \log(p)$ for convenience as in the previous case and α is some parameter ≥ 10. We estimate the error term $R := S_2 - S_2'$ by applying Lemma 2.2.27 with $Q = 4p$. Similarly to the approach in the previous case this yields the estimate

$$\begin{aligned} R \ll_\alpha \frac{(\log z)}{z^\alpha} & \sum_{\substack{p^- < q < p^+ \\ \mathrm{disc}(\mathbb{Q}(\sqrt{D(p,q)})) \notin \mathcal{E}(4p)}} \sum_{\substack{f \mid D(p,q) \\ (f,2)=1}} \frac{1}{\varphi(f)} \\ + & \sum_{\substack{p^- < q < p^+ \\ \mathrm{disc}(\mathbb{Q}(\sqrt{D(p,q)})) \in \mathcal{E}(4p)}} \sum_{\substack{f \mid D(p,q) \\ (f,2)=1}} \frac{z}{\varphi(f)}. \end{aligned}$$

For each $q \in (p^-, p^+)$ if $\Delta := \mathrm{disc}(\mathbb{Q}(\sqrt{D(p,q)})) \in \mathcal{E}(4p)$ we have that $D(p,q) = \Delta m^2$ for some $m \in \mathbb{N}$, or equivalently $(p+1-q)^2 - \Delta m^2 = 4p$. So, for each fixed $\Delta \in \mathcal{E}(4p)$ there are at most $\tau(4p) = 6$ admissible values of q. Thus,

$$\#\{p^- < q < p^+ : \mathrm{disc}(\mathbb{Q}(\sqrt{D(p,q)})) \in \mathcal{E}(4p)\} \leq \#\mathcal{E}(4p)\tau(4p) \ll p^{\frac{1}{5}},$$

since $\alpha \geq 10$. From the properties of the Euler φ-function in Theorem 2.2.5 we have that

$$\begin{aligned} \sum_{\substack{f \mid D(p,q) \\ (f,2)=1}} \frac{1}{\varphi(f)} \ll \log z \sum_{\substack{f \mid D(p,q) \\ (f,2)=1}} \frac{1}{f} = \log z \prod_{\substack{\ell \mid D(p,q) \\ \ell \neq 2}} \left(1 - \frac{1}{\ell}\right)^{-1} \\ \leq \log z \frac{D(p,q)}{\varphi(D(p,q))} \ll (\log z)^2. \end{aligned}$$

Combining the above estimates gives

$$R \ll_\alpha \frac{\sqrt{p}(\log z)^2}{z^\alpha} + p^{\frac{1}{5}} z(\log z)^2$$

and hence the remainder term is smaller thant he main term in (4.37) (since $\alpha \geq 10$). Now we bound S_2' as before and from Mertens' Theorem and following as in (4.8), (4.9) and (4.10) we have that

$$L(1, \chi; z^{8\alpha^2}) \ll \frac{f}{\varphi(f)} \prod_{\ell \leq \sqrt{z}} \left(1 + \frac{\left(\frac{D(p,q)}{\ell}\right)}{\ell}\right). \tag{4.38}$$

From (4.38) we have that

$$S_2' \ll \sum_{p^- < q < p^+} \prod_{\ell \leq \sqrt{z}} \left(1 + \frac{\left(\frac{D(p,q)}{\ell}\right)}{\ell}\right) \sum_{\substack{f | D(p,q) \\ (f,2)=1}} \frac{f}{\varphi^2(f)}, \tag{4.39}$$

and similarly to the computation in (4.14) we have that

$$\sum_{\substack{f | D(p,q) \\ (f,2)=1}} \frac{f}{\varphi^2(f)} = \prod_{\substack{\ell | D(p,q) \\ \ell \neq 2}} \left(1 + \frac{\ell^2}{(\ell-1)^3}\right) \ll \sum_{\substack{f | D(p,q) \\ P^+(f) \leq \sqrt{z}}} \frac{\mu^2(f)}{f}. \tag{4.40}$$

Now we swap the sum over f in (4.40) with the product over ℓ in (4.39) which gives

$$\begin{aligned} S_2' &\ll \sum_{p^- < q < p^+} \sum_{\substack{f | D(p,q) \\ (f,2)=1 \\ P^+(f) \leq \sqrt{z}}} \frac{\mu^2(f)}{f} \prod_{\substack{\ell \leq \sqrt{z} \\ \ell \nmid 2f}} \left(1 + \frac{\left(\frac{D(p,q)}{\ell}\right)}{\ell}\right) \\ &= \sum_{\substack{P^+(f) \leq \sqrt{z} \\ (f,2)=1}} \frac{\mu^2(f)}{f} \sum_{\substack{p^- < q < p^+ \\ f | D(p,q)}} \prod_{\substack{\ell \leq \sqrt{z} \\ \ell \nmid 2f}} \left(1 + \frac{\left(\frac{D(p,q)}{\ell}\right)}{\ell}\right). \end{aligned} \tag{4.41}$$

As in the previous case we have that

$$\prod_{\substack{\ell\leq\sqrt{z}\\ \ell\nmid 2f}}\left(1+\frac{\left(\frac{D(p,q)}{\ell}\right)}{\ell}\right)=\sum_{\substack{P^+(n)\leq\sqrt{z}\\(n,2f)=1}}\frac{\mu^2(n)}{n}\left(\frac{D(p,q)}{n}\right), \tag{4.42}$$

and as in the previous case we require q coprime to $2fn$ so the RHS of (4.41) becomes

$$\begin{aligned}
&\sum_{\substack{P^+(f)\leq\sqrt{z}\\(f,2)=1}}\frac{\mu^2(f)}{f}\sum_{\substack{p^-<q<p^+\\ f|D(p,q)}}\prod_{\substack{\ell\leq\sqrt{z}\\ \ell\nmid 2f}}\left(1+\frac{\left(\frac{D(p,q)}{\ell}\right)}{\ell}\right)\\
&=\sum_{\substack{P^+(f)\leq\sqrt{z}\\(f,2)=1}}\frac{\mu^2(f)}{f}\sum_{\substack{P^+(n)\leq\sqrt{z}\\(n,2f)=1}}\frac{\mu^2(n)}{n}\sum_{\substack{p^-<q<p^+\\ f|D(p,q)\\(q,2fn)=1}}\left(\frac{D(p,q)}{n}\right)\\
&+\sum_{\substack{P^+(f)\leq\sqrt{z}\\(f,2)=1}}\frac{\mu^2(f)}{f}\sum_{\substack{P^+(n)\leq\sqrt{z}\\(n,2f)=1}}\frac{\mu^2(n)}{n}\sum_{\substack{p^-<q<p^+\\ f|D(p,q)\\ q|2fn}}\left(\frac{D(p,q)}{n}\right).
\end{aligned}\tag{4.43}$$

As in the previous case we have that the second term in (4.43) is bounded by

$$\begin{aligned}
&\sum_{\substack{P^+(f)\leq\sqrt{z}\\(f,2)=1}}\frac{\mu^2(f)}{f}\sum_{\substack{P^+(n)\leq\sqrt{z}\\(n,2f)=1}}\frac{\mu^2(n)}{n}\sum_{\substack{p^-<q<p^+\\ f|D(p,q)\\ q|2fn}}\left(\frac{D(p,q)}{n}\right)\\
&\ll\sum_{\substack{P^+(f)\leq\sqrt{z}\\(f,2)=1}}\frac{\mu^2(f)\tau(f)}{f}\sum_{\substack{P^+(n)\leq\sqrt{z}\\(n,2f)=1}}\frac{\mu^2(n)\tau(n)}{n}\ll z^{\epsilon}\log^2 z
\end{aligned}$$

for some $\epsilon>0$, which is smaller than the main term. Hence,

$$S_2'\ll\sum_{\substack{P^+(f)\leq\sqrt{z}\\(f,2)=1}}\frac{\mu^2(f)}{f}\sum_{\substack{P^+(n)\leq\sqrt{z}\\(n,2f)=1}}\frac{\mu^2(n)}{n}\sum_{\substack{p^-<q<p^+\\ f|D(p,q)\\(q,2fn)=1}}\left(\frac{D(p,q)}{n}\right). \tag{4.44}$$

As in the previous case we use the fundamental lemma for the combinatorial sieve, Lemma 2.2.28 with $y=p^{\frac{1}{6}}$ and $D=y^2$ to bound the innermost sum of (4.41). So we extend the summation from primes q to integers m with no prime factors $\leq y$. Conse-

quently,

$$S_2' \leq S_3 := \sum_{\substack{P^+(f)\leq\sqrt{z}\\(f,2)=1}} \frac{\mu^2(f)}{f} \sum_{\substack{P^+(n)\leq\sqrt{z}\\(n,2f)=1}} \frac{\mu^2(n)}{n} \sum_{\substack{p^-<m<p^+\\f|D(p,m)\\(m,2fn)=1}} (\lambda^+ * 1)(m) \left(\frac{D(p,m)}{n}\right), \tag{4.45}$$

by the positivity of the Euler product in (4.42).

Since λ^+ is supported on integers $a \mid m, a \leq D, (m, 2fn) = 1$, we have that (4.45) becomes

$$\begin{aligned} S_3 &= \sum_{\substack{P^+(f)\leq\sqrt{z}\\(f,2)=1}} \frac{\mu^2(f)}{f} \sum_{\substack{P^+(n)\leq\sqrt{z}\\(n,2f)=1}} \frac{\mu^2(n)}{n} \sum_{\substack{a\leq N\\(a,2fn)=1}} \lambda^+(a) \sum_{\substack{p^-<m<p^+\\f|D(p,m),a|m}} \left(\frac{D(p,m)}{n}\right) \\ &= \sum_{\substack{P^+(f)\leq\sqrt{z}\\(f,2)=1}} \frac{\mu^2(f)}{f} \sum_{\substack{P^+(n)\leq\sqrt{z}\\(n,2f)=1}} \frac{\mu^2(n)}{n} \sum_{\substack{a\leq D\\(a,2fn)=1}} \lambda^+(a) \sum_{b\in\mathbb{Z}/n\mathbb{Z}} \left(\frac{b}{n}\right) S(a,f,n,b), \end{aligned} \tag{4.46}$$

by splitting the integers in the interval $m \in (p^-, p^+)$ according to the congruence class of $D(p,m) \pmod n$, where

$$S(a,f,n,b) = \#\left\{ \begin{array}{ll} p^- < m < p^+ & D(p,m) \equiv 0 \pmod f \\ m \equiv 0 \pmod a & D(p,m) \equiv b \pmod n \end{array} \right\}.$$

Let $\Delta(m) := D(p,m)$ then we have that

$$S(a,f,n,b) = \left(\frac{4\sqrt{p}}{afn}\right) T(a,f,n,b) + O(T(a,f,n,b)), \tag{4.47}$$

where

$$T(a,f,n,b) = \#\left\{ m \in \mathbb{Z}/afn\mathbb{Z} : \begin{array}{l} \Delta(m) \equiv 0 \pmod f \\ \Delta(m) \equiv b \pmod n \\ m \equiv 0 \pmod a \end{array} \right\}.$$

Since a, f, n are all coprime and the sum in (4.47) is only over square-free numbers, by

the Chinese remainder theorem, we have as in the previous case that

$$T(a,f,n,b) = h_1(f,0)h_1(n,b)$$

where $h_1(u,v)$ is defined in (4.29). Combining (4.46) and (4.47) gives

$$S_3 = 4\sqrt{p} \sum_{\substack{P^+(f)\leq\sqrt{z}\\(f,2)=1}} \frac{\mu^2(f)h_1(f,0)}{f^2} \sum_{\substack{P^+(n)\leq\sqrt{z}\\(n,2f)=1}} \frac{\mu^2(n)}{n^2} \sum_{\substack{a\leq D\\(a,2fn)=1}} \frac{\lambda^+(a)}{a} \sum_{b\in\mathbb{Z}/n\mathbb{Z}} \left(\frac{b}{n}\right) h_1(n,b)$$
$$+ O\left(\sum_{\substack{P^+(f)\leq\sqrt{z}\\(f,2)=1}} \frac{\mu^2(f)\tau(f)}{f} \sum_{\substack{P^+(n)\leq\sqrt{z}\\(n,2f)=1}} \frac{\mu^2(n)}{n} \sum_{\substack{a\leq D\\(a,2fn)=1}} \sum_{b\in\mathbb{Z}/n\mathbb{Z}} \tau(n) \right). \tag{4.48}$$

The second term on the RHS of (4.48) is bounded by

$$\ll D \sum_{\substack{P^+(f)\leq\sqrt{z}\\(f,2)=1}} \frac{\mu^2(f)\tau(f)}{f} \sum_{\substack{P^+(n)\leq\sqrt{z}\\(n,2f)=1}} \mu^2(n)\tau(n).$$

We have by Mertens' Theorem, Theorem 2.2.26 and Theorem 2.2.6 that

$$\sum_{\substack{P^+(n)\leq\sqrt{z}\\(n,2f)=1}} \mu^2(n)\tau(n) \ll \frac{\sqrt{z}}{\log z} \prod_{p\leq z} \left(1+\frac{2}{p}\right) \ll \sqrt{z}\log z,$$
$$\sum_{\substack{P^+(f)\leq\sqrt{z}\\(f,2)=1}} \frac{\mu^2(f)\tau(f)}{f} \ll \frac{\sqrt{z}}{\log z} \prod_{p\leq z} \left(1+\frac{2}{p^2}\right) \ll \frac{\sqrt{z}}{\log z}.$$

Therefore, the second term in (4.48) is $\ll Dz$. As in the previous case we set

$$c(n) := \sum_{b\in\mathbb{Z}/n\mathbb{Z}} \left(\frac{b}{n}\right) h_1(n,b),$$

then from Lemma 2.2.28 and Mertens' Theorem, Theorem 2.2.26 we have that (4.48)

becomes

$$S_3 \ll \sqrt{p} \sum_{\substack{P^+(f)\leq\sqrt{z}\\(f,2)=1}} \frac{\mu^2(f)\tau(f)}{f^2} \sum_{\substack{P^+(n)\leq\sqrt{z}\\(n,2f)=1}} \frac{\mu^2(n)|c(n)|}{n^2} \prod_{\substack{\ell\leq y\\ \ell\nmid 2fn}} \left(1-\frac{1}{\ell}\right) + Dz.$$
$$\ll \frac{\sqrt{p}}{\log y} \sum_{\substack{P^+(f)\leq\sqrt{z}\\(f,2)=1}} \frac{\mu^2(f)\tau(f)}{f\varphi(f)} \sum_{\substack{P^+(n)\leq\sqrt{z}\\(n,2f)=1}} \frac{\mu^2(n)|c(n)|}{n\varphi(n)} + Dz. \tag{4.49}$$

In the previous case we showed that $c(n)$ is a multiplicative function and

$$c(\ell) = \begin{cases} \ell - 1 & \text{if } 16p^2 \equiv 0 \pmod{\ell}, \\ -1 & \text{if } 16p^2 \not\equiv 0 \pmod{\ell}. \end{cases}$$

Since $P^+(n) \leq \sqrt{z} := \sqrt{\log p} < p$ we have that $c(n) = -1$ and thus,

$$\sum_{\substack{P^+(n)\leq\sqrt{z}\\(n,2f)=1}} \frac{\mu^2(n)|c(n)|}{n\varphi(n)} \ll \sum_{\substack{P^+(n)\leq\sqrt{z}\\(n,2f)=1}} \frac{\mu^2(n)(\log\log n)^2}{n^2} \ll 1,$$

and by the bounds on the Euler φ-function in Theorem 2.2.5 we have that

$$\sum_{\substack{P^+(f)\leq\sqrt{z}\\(f,2)=1}} \frac{\mu^2(f)\tau(f)}{f^2} \ll \sum_{\substack{P^+(f)\leq\sqrt{z}\\(f,2)=1}} \frac{\mu^2(f)\tau(f)\log\log f}{f^2} \ll 1.$$

Thus,

$$S_2 \ll S_2' \ll S_3 \ll \frac{\sqrt{p}}{\log y} + D\log^2 p \ll \frac{\sqrt{p}}{\log p},$$

for $y = p^{\frac{1}{6}}, D = (p^{\frac{1}{6}})^2 = p^{\frac{1}{3}}$, which completes the proof. □

Chapter 5

Length of the average

5.1 A short length of the average

In this chapter we will show how the technique of multiplicative character sums used by Baier, in [Ba1], Balog, Cojocaru and David in [BCD] and by Banks and Shparlinski in [BanShp] generalizes to the case of aliquot cycles to give a short length for the average given in Theorem 1.0.5.

As in Chapter 3 we define the following vectors of integers

$$P := (p_1, \dots, p_L), \quad S := (s_1, \dots, s_L), \quad T := (t_1, \dots, t_L), \quad U := (u_1, \dots, u_L),$$

where $(p_1, \dots, p_L)$ are distinct primes. We also recall the definitions

$$w(P,S,T) = \begin{cases} 1 & \text{if } \#E_{s_i,t_i}(\mathbb{F}_{p_i}) = p_{i+1} \text{ for } 1 \le i \le L, \\ 0 & \text{otherwise,} \end{cases}$$

and the sum $R(P,S,T)$, which is the number of integers $|a| \le A, |b| \le B$ such that there exist $U \in \mathbb{F}(P)^*$ satisfying

$$a \equiv s_i u_i^4 \pmod{p_i}, \quad b \equiv t_i u_i^6 \pmod{p_i} \quad \text{for } 1 \le i \le L.$$

The goal of this section is to prove Lemma 3.2.2, which we restate below.

Lemma 5.1.1. *Fix an integer $L \geq 2$, let $E/\mathbb{Q}$ be an elliptic curve, let $A, B > 0$ then for any positive integer k, we have that as $X \to \infty$,*

$$\sum_{\substack{p \leq X \\ p_i^- < p_{i+1} < p_i^+ \\ 1 \leq i \leq L-1}} \frac{1}{p_1 \cdots p_L} \sum_{S,T \in \mathbb{F}(P)^*} w(P,S,T) \left(R(P,S,T) - \frac{AB}{2^{L-2} p_1 \cdots p_L} \right)$$

$$\ll_{k,L} ABX^{\frac{1}{2}-\frac{1}{4k}} (\log X)^{\frac{L-1}{2k}} (\log\log X)^L \log^{\frac{k^2-1}{2k}} AB$$

$$+ (A\sqrt{B} + B\sqrt{A}) X^{\frac{1}{2}+\frac{3L-1}{4k}} (\log X)^{\frac{k^2+L-1}{2k}} (\log\log X)^L + \sqrt{AB} X^{\frac{3L+2}{4}} (\log X)^{3-L}. \quad (5.1)$$

Proof. Let χ_i, χ_i' be Dirichlet characters modulo p_i for $1 \leq i \leq L$. Throughout this section χ_0 denotes the principal character modulo n for any integer n and $\overline{\chi}$ denotes the complex conjugate of χ. We also define the following sums of characters,

$$\mathcal{A}(\chi) := \sum_{|a| \leq A} \chi(a) \quad \text{and} \quad \mathcal{B}(\chi) := \sum_{|b| \leq B} \chi(b).$$

Let S, T, a, b be fixed. If there exists a $u_i \pmod{p_i}$ such that $a \equiv s_i u_i^4 \pmod{p_i}$ and $b \equiv t_i u_i^6 \pmod{p_i}$ then there exists exactly two such u_i, namely $\pm u_i$. To ease notation, unless otherwise stated, we define

$$\chi := \chi_1 \cdots \chi_L \quad \text{and} \quad \chi' := \chi_1' \cdots \chi_L'.$$

Since Dirichlet characters are completely multiplicative we have that

$$\begin{aligned}
R(P,S,T) = & \sum_{\substack{|a|\le A,|b|\le B\\ U\in\mathbb{F}(P)^*\\ a\equiv s_iu_i^4 \pmod{p_i},b\equiv t_iu_i^6 \pmod{p_i}\\ 1\le i\le L}} 1\\
=&\frac{1}{2^L}\sum_{\substack{|a|\le A\\|b|\le B}}\sum_{U\in\mathbb{F}(P)^*}\prod_{i=1}^{L}\left(\frac{1}{(p_i-1)^2}\sum_{\chi_i \pmod{p_i}}\chi_i(s_iu_i^4)\overline{\chi_i}(a)\sum_{\chi_i' \pmod{p_i}}\chi_i'(t_iu_i^6)\overline{\chi_i'}(b)\right)\\
=&\frac{1}{2^L}\prod_{i=1}^{L}\left(\frac{1}{(p_i-1)^2}\sum_{\substack{\chi_i \pmod{p_i}\\ \chi_i' \pmod{p_i}}}\chi_i(s_i)\chi_i'(t_i)\sum_{U\in\mathbb{F}(P)^*}\chi_i(u_i^4)\chi_i'(u_i^6)\right)\\
&\times\sum_{\substack{|a|\le A\\|b|\le B}}\overline{\chi_1\cdots\chi_L}(a)\overline{\chi_1'\cdots\chi_L'}(b). \qquad (5.2)
\end{aligned}$$

By the orthogonality of Dirichlet characters, Theorem 2.2.17 we have that the sum over U becomes

$$\begin{aligned}
\sum_{U\in\mathbb{F}(P)^*}\chi_i(u_i^4)\chi_i'(u_i^6) &= \sum_{u_1\in\mathbb{F}_{p_1}^*}\chi_1^4(u_1)\chi_1'^6(u_1)\cdots\sum_{u_L\in\mathbb{F}_{p_L}^*}\chi_L^4(u_L)\chi_L'^6(u_L)\\
&= \begin{cases}\prod_{i=1}^{L}(p_i-1) & \text{if } \chi_i^4\chi_i'^6=\chi_0 \pmod{p_i} \text{ for } 1\le i\le L,\\ 0 & \text{otherwise.}\end{cases} \qquad (5.3)
\end{aligned}$$

Hence, we have from (5.2) and (5.3) that

$$\begin{aligned}
R(P,S,T) =&\frac{1}{2^L}\prod_{i=1}^{L}\left(\frac{1}{p_i-1}\sum_{\chi_i^4\chi_i'^6=\chi_0 \pmod{p_i}}\chi_i(s_i)\chi_i'(t_i)\right)\mathcal{A}(\overline{\chi})\mathcal{B}(\overline{\chi'})\\
=&\frac{1}{2^L}\sum_{\substack{\chi_1,\dots,\chi_L\\ \chi_i',\dots,\chi_L'\\ \chi_i^4(\chi_i')^6=\chi_0 \pmod{p_i}}}\prod_{i=1}^{L}\left(\frac{1}{p_i-1}\chi_i(s_i)\chi_i'(t_i)\right)\mathcal{A}(\overline{\chi})\mathcal{B}(\overline{\chi'}). \qquad (5.4)
\end{aligned}$$

We have that (5.4) can be broken up into four types of sums which we define below.

$$\begin{cases} R_1(P,S,T) & \text{if } \chi_i = \chi_i' = \chi_0 \pmod{p_i} \text{ for } 1 \le i \le L, \\ R_2(P,S,T) & \text{if } \chi_i = \chi_0 \pmod{p_i} \text{ for } 1 \le i \le L \text{ and } \chi_i' \ne \chi_0 \pmod{p_i} \text{ for some } i, \\ R_3(P,S,T) & \text{if } \chi_i' = \chi_0 \pmod{p_i} \text{ for } 1 \le i \le L \text{ and } \chi_i \ne \chi_0 \pmod{p_i} \text{ for some } i, \\ R_4(P,S,T) & \text{otherwise.} \end{cases}$$

Hence, we can express (5.4) as

$$R(P,S,T) = \sum_{1 \le j \le 4} R_j(P,S,T). \tag{5.5}$$

For $j = 1$ since $\chi_i = \chi_i' = \chi_0 \pmod{p_i}$ is the trivial character for $1 \le i \le L$, we have that

$$\begin{aligned} \mathcal{A}(\overline{\chi}) &= \sum_{|a| \le A} \overline{\chi}(a) = \sum_{|a| \le A} \chi_0(a) \\ &= \sum_{\substack{|a| \le A \\ p_1 \cdots p_L \nmid a}} 1 = 2A\left(1 - \frac{1}{p_1 \cdots p_L}\right) + O(1) \end{aligned}$$

and similarly,

$$\mathcal{B}(\overline{\chi'}) = 2B\left(1 - \frac{1}{p_1 \cdots p_L}\right) + O(1).$$

Thus, we have that the contribution to the RHS of (5.5) is

$$R_1(P,S,T) = \frac{AB}{2^{L-2} p_1 \cdots p_L} + O_L\left(\frac{AB}{p^{L+1}} + \frac{A+B+1}{p^L}\right). \tag{5.6}$$

Recall from (3.18) in Lemma 3.15 that

$$\sum_{S,T \in \mathbb{F}(P)^*} w(P,S,T) = p^L \prod_{i=1}^{L} H(D(p_i, p_{i+1})) + O\left(p^{\frac{3L-1}{2}} (\log p)^L (\log\log p)^L\right). \tag{5.7}$$

Hence, we can plug (5.6) into the LHS of (5.1) and using the bound in (5.7) we have that

$$\begin{aligned}
&\sum_{\substack{p\leq X\\ p_i^-<p_{i+1}<p_i^+\\ 1\leq i\leq L-1}} \frac{1}{p_1\cdots p_L}\sum_{S,T\in\mathbb{F}(P)^*} w(P,S,T)S_1(P,S,T)\\
=&\frac{AB}{2^{L-2}}\sum_{\substack{p\leq X\\ p_i^-<p_{i+1}<p_i^+\\ 1\leq i\leq L-1}} \frac{1}{p_1^2\cdots p_L^2}\sum_{S,T\in\mathbb{F}(P)^*} w(P,S,T)\\
&+O_L\left(\sum_{p\leq X}\left(\frac{AB}{p^{L+1}}+\frac{A+B}{p^L}\right)\sum_{\substack{p_i^-<p_{i+1}<p_i^+\\ 1\leq i\leq L-1}}\prod_{j=1}^{L}H(D(p_j,p_{j+1}))\right). \qquad (5.8)
\end{aligned}$$

By partial summation, Proposition 3.2.3 and Proposition 3.2.4 we have for the error term in (5.8) that

$$\begin{aligned}
&\sum_{p\leq X}\left(\frac{AB}{p^{L+1}}+\frac{A+B}{p^L}\right)\sum_{\substack{p_i^-<p_{i+1}<p_i^+\\ 1\leq i\leq L-1}}\prod_{j=1}^{L}H(D(p_j,p_{j+1}))\\
\ll_L&\sum_{p\leq X}\left(\frac{AB}{p^{L+1}}+\frac{A+B}{p^L}\right)\frac{p^{L-\frac{1}{2}}}{\log^{L-1}p}\ll_L AB+\frac{(A+B)\sqrt{X}}{\log^L X}. \qquad (5.9)
\end{aligned}$$

We have that (5.9) is smaller than that of the first two terms on the RHS in the error term of (5.1) so it is a lower order error term.

For $j=2$ we have to sum over all characters such that $\chi_i=\chi_0 \pmod{p_i}$ for $1\leq i\leq L$ and there exists a $j\in[1,L]$ such that $\chi_j'\neq\chi_0 \pmod{p_j}$, which we express as the following sum

$$\begin{aligned}
R_2(P,S,T)&=2A\left(1-\frac{1}{p_1\cdots p_L}\right)\frac{1}{2^L}\prod_{i=1}^{L}\frac{1}{p_i-1}\sum_{\substack{(\chi')^6=\chi_0 \pmod{p_1\cdots p_L}\\ \chi'\neq\chi_0 \pmod{p_1\cdots p_L}}}\mathcal{B}(\overline{\chi'})\\
&\ll\frac{A}{p_1\cdots p_L}\sum_{\substack{(\chi')^6=\chi_0 \pmod{p_1\cdots p_L}\\ \chi'\neq\chi_0 \pmod{p_1\cdots p_L}}}|\mathcal{B}(\chi')|,
\end{aligned}$$

and similarly, for $j = 3$ we have that

$$R_3(P,S,T) \ll \frac{B}{p_1 \cdots p_L} \sum_{\substack{\chi^4 = \chi_0 \pmod{p_1 \cdots p_L} \\ \chi \neq \chi_0 \pmod{p_1 \cdots p_L}}} |\mathcal{A}(\chi)|.$$

These estimates are independent of S and T, so for $2 \leq j \leq 3$ we can plug (5.6) into the LHS of (5.1) and use the bound from (5.7) to obtain

$$\begin{aligned}
&\sum_{\substack{p \leq X \\ p_i^- < p_{i+1} < p_i^+ \\ 1 \leq i \leq L-1}} \frac{1}{p_1 \cdots p_L} \sum_{S,T \in \mathbb{F}(P)^*} w(P,S,T) \left| \sum_{2 \leq j \leq 3} R_j(P,S,T) \right| \\
&\ll \sum_{\substack{p \leq X \\ p_i^- < p_{i+1} < p_i^+ \\ 1 \leq i \leq L-1}} \frac{1}{p_1 \cdots p_L} \prod_{j=1}^{L} H(D(p_j, p_{j+1})) \\
&\times \left(A \sum_{\substack{(\chi')^6 = \chi_0 \pmod{p_1 \cdots p_L} \\ \chi' \neq \chi_0 \pmod{p_1 \cdots p_L}}} |\mathcal{B}(\chi')| + B \sum_{\substack{\chi^4 = \chi_0 \pmod{p_1 \cdots p_L} \\ \chi \neq \chi_0 \pmod{p_1 \cdots p_L}}} |\mathcal{A}(\chi)| \right). \qquad (5.10)
\end{aligned}$$

For the sake of clarity, we will first give a bound for

$$A \sum_{\substack{p \leq X \\ p_i^- < p_{i+1} < p_i^+ \\ 1 \leq i \leq L-1}} \frac{1}{p_1 \cdots p_L} \prod_{j=1}^{L} H(D(p_j, p_{j+1})) \sum_{\substack{(\chi')^6 = \chi_0 \pmod{p_1 \cdots p_L} \\ \chi' \neq \chi_0 \pmod{p_1 \cdots p_L}}} |\mathcal{B}(\chi')|$$

in (5.10) in the $L = 2$ case such that $\chi_2' \neq \chi_0 \pmod{p_2}$. We then generalize the argument to all L. In this case we have that the first sum in (5.10) can be expressed as

$$A \sum_{\substack{p \leq X \\ p^- < q < p^+}} \frac{H(D(p,q))^2}{pq} \sum_{\substack{(\chi_1' \chi_2')^6 = \chi_0 \pmod{pq} \\ \chi_1' \chi_2' \neq \chi_0 \pmod{pq}}} \left| \sum_{b \leq B} \chi_1' \chi_2'(b) \right|. \qquad (5.11)$$

We have two cases to consider. Either $\chi_1' \neq \chi_0 \pmod{p}$, in which case $\chi_1' \chi_2'$ is primitive, or $\chi_1' = \chi_0 \pmod{p}$, in which case $\chi_1' \chi_2'$ is imprimitive.

We will consider the case when $\chi_1'\chi_2'$ is primitive first. In this case, the sum

$$\sideset{}{^*}\sum_{\substack{p\leq X\\ p^-<q<p^+\\ \chi'\neq\chi_0 \pmod{pq}}}$$

denotes the sum over p, q and over characters $\chi' = \chi_1'\chi_2'$ where $\chi_1' \neq \chi_0 \pmod{p}$ and $\chi_2' \neq \chi_0 \pmod{q}$. Since there are a bounded number of characters satisfying $(\chi_1'\chi_2')^6 = \chi_0 \pmod{pq}$, from Hölder's inequality we have that the sum on the RHS of (5.11) becomes

$$\begin{aligned} &A \sum_{\substack{p\leq X\\ p^-<q<p^+}} \frac{H(D(p,q))^2}{pq} \sum_{\substack{(\chi_1'\chi_2')^6=\chi_0 \pmod{pq}\\ \chi_1'\chi_2'\neq\chi_0 \pmod{pq}}} \left|\sum_{b\leq B} \chi_1'\chi_2'(b)\right| \\ \ll &A \left(\sideset{}{^*}\sum_{\substack{p\leq X\\ p^-<q<p^+\\ \chi'\neq\chi_0 \pmod{pq}}} \left(\frac{H(D(p,q))^2}{pq}\right)^{\frac{2k}{2k-1}}\right)^{1-\frac{1}{2k}} \left(\sideset{}{^*}\sum_{\substack{p\leq X\\ p^-<q<p^+\\ \chi'\neq\chi_0 \pmod{pq}}} \left|\sum_{b\leq B}\chi'(b)\right|^{2k}\right)^{\frac{1}{2k}}. \end{aligned} \tag{5.12}$$

We recall that

$$H(D(p_i, p_{i+1})) \ll \sqrt{p}\log p \log\log p,$$

from (3.7) and therefore the first product in (5.12) becomes

$$\begin{aligned} \left(\sideset{}{^*}\sum_{\substack{p\leq X\\ p^-<q<p^+\\ \chi'\neq\chi_0 \pmod{pq}}} \left(\frac{H(D(p,q))^2}{pq}\right)^{\frac{2k}{2k-1}}\right)^{1-\frac{1}{2k}} &\ll \left(\sum_{\substack{p\leq X\\ p^-<q<p^+}} \left(\frac{(\log p)^2(\log\log p)^2}{p}\right)^{\frac{2k}{2k-1}}\right)^{1-\frac{1}{2k}} \\ &\ll \left(\sum_{p\leq X} \frac{\sqrt{p}}{\log p}\left(\frac{(\log p)^2(\log\log p)^2}{p}\right)^{\frac{2k}{2k-1}}\right)^{1-\frac{1}{2k}} \\ &\ll X^{\frac{1}{2}-\frac{3}{4k}}(\log X)^{\frac{1}{k}}(\log\log X)^2. \end{aligned} \tag{5.13}$$

We can rewrite

$$\left|\sum_{b\leq B}\chi'(b)\right|^{2k} = \left|\sum_{b\leq B^k}\tau_k(b;B)\chi'(b)\right|^2, \tag{5.14}$$

where $\tau_k(b;B)$ is the number of ways of writing b as the product of k positive integers at most B. We extend the sum in the second product in (5.12) to a sum over all primitive characters modulo d for all modulus $d \leq Q = X^2$, since $pq \ll X^2$ and we use the large sieve inequality, Theorem 2.2.22, which gives

$$\begin{aligned}
\left(\sum_{\substack{p\leq X\\ p^-<q<p^+\\ \chi'\neq\chi_0 \pmod{pq}}}^{*}\left|\sum_{b\leq B}\chi'(b)\right|^{2k}\right)^{\frac{1}{2k}} &\ll \left(\sum_{\substack{p\leq X\\ p^-<q<p^+\\ \chi'\neq\chi_0 \pmod{pq}}}^{*}\left|\sum_{b\leq B^k}\tau_k(b;B)\chi'(b)\right|^2\right)^{\frac{1}{2k}}\\
&\ll \left(\sum_{\substack{d\leq X^2\\ \chi \pmod d\\ \chi \text{ primitive}}}\left|\sum_{b\leq B^k}\tau_k(b;B)\chi(b)\right|^2\right)^{\frac{1}{2k}}\\
&\ll \left(\sum_{\substack{d\leq X^2\\ \chi \pmod d\\ \chi \text{ primitive}}}\left|\sum_{b\leq B^k}\tau_k(b)\chi(b)\right|^2\right)^{\frac{1}{2k}}\\
&\ll \left((B^k+X^4)\sum_{b\leq B^k}|\tau_k(b)|^2\right)^{\frac{1}{2k}}\\
&\ll \left((B^k+X^4)B^k\log^{k^2-1}(B^k)\right)^{\frac{1}{2k}},
\end{aligned} \tag{5.15}$$

where we used Theorem 2.2.6 to bound $\tau_k(b)$. Combining (5.12), (5.13) and (5.15) gives

$$\begin{aligned}
&A\sum_{\substack{p\leq X\\ p^-<q<p^+}}\frac{H(D(p,q))^2}{pq}\sum_{\substack{(\chi_1'\chi_2')^6=\chi_0 \pmod{pq}\\ \chi_1'\chi_2'\neq\chi_0 \pmod{pq}}}\left|\sum_{b\leq B}\chi_1'\chi_2'(b)\right|\\
\ll& A\left((B^k+X^4)B^k\log^{k^2-1}(B^k)\right)^{\frac{1}{2k}}X^{\frac{1}{2}-\frac{3}{4k}}(\log X)^{\frac{1}{k}}(\log\log X)^2.
\end{aligned} \tag{5.16}$$

Suppose that $B^k > X^4$ then we have that the RHS of (5.15) becomes

$$\left((B^k + X^4)B^k \log^{k^2-1}(B^k)\right)^{\frac{1}{2k}} \ll_k B \log^{\frac{k^2-1}{2k}} B, \tag{5.17}$$

for $k \geq 1$. Then suppose that $B^k \leq X^4$ for all $k \geq 1$. Then we can replace $\log B$ by $\log X$ in (5.15), which gives

$$\left((B^k + X^4)B^k \log^{k^2-1}(B^k)\right)^{\frac{1}{2k}} \ll_k \sqrt{B} X^{\frac{2}{k}} \log^{\frac{k^2-1}{2k}}(X). \tag{5.18}$$

Since

$$(B^k + X^4)^{\frac{1}{2k}} \ll_k \sqrt{B} + X^{\frac{2}{k}},$$

combining (5.17) and (5.18) with (5.16) gives

$$\begin{aligned} & A \sum_{\substack{p \leq X \\ p^- < q < p^+}} \frac{H(D(p,q))^2}{pq} \sum_{\substack{(\chi_1'\chi_2')^6 = \chi_0 \pmod{pq} \\ \chi_1'\chi_2' \neq \chi_0 \pmod{pq}}} \left| \sum_{b \leq B} \chi_1'\chi_2'(b) \right| \\ \ll_k & A \left((B^k + X^4)B^k \log^{k^2-1}(B^k)\right)^{\frac{1}{2k}} X^{\frac{1}{2} - \frac{3}{4k}} (\log X)^{\frac{1}{k}} (\log\log X)^2 \\ = & ABX^{\frac{1}{2} - \frac{3}{4k}} (\log X)^{\frac{1}{k}} (\log\log X)^2 \log^{\frac{k^2-1}{2k}} B + A\sqrt{B} X^{\frac{1}{2} + \frac{5}{4k}} (\log X)^{\frac{k^2+1}{2k}} (\log\log X)^2. \end{aligned} \tag{5.19}$$

We now consider the imprimitive case. Fix $p \leq X$ and $\chi_1' = \chi_0 \pmod p, \chi_2' \neq \chi_0 \pmod q$. In this case, the sum

$$\sum_{\substack{p^- < q < p^+ \\ \chi_2' \neq \chi_0 \pmod q}}^{*}$$

denotes the sum over q and over characters χ_2' where $\chi_2' \neq \chi_0 \pmod q$. As in the primitive

case, from Hölder's inequality we have that (5.11) becomes

$$A \sum_{\substack{p\leq X \\ p^-<q<p^+}} \frac{H(D(p,q))^2}{pq} \sum_{\substack{(\chi_1'\chi_2')^6=\chi_0 \pmod{pq} \\ \chi_1'\chi_2'\neq\chi_0 \pmod{pq}}} \left|\sum_{b\leq B} \chi_1'\chi_2'(b)\right|$$

$$\ll A \sum_{p\leq X} \left(\sum_{\substack{p^-<q<p^+ \\ \chi_2'\neq\chi_0 \pmod q}}^{*} \left(\frac{H(D(p,q))^2}{pq}\right)^{\frac{2k}{2k-1}} \right)^{1-\frac{1}{2k}} \left(\sum_{\substack{p^-<q<p^+ \\ \chi_2'\neq\chi_0 \pmod q}}^{*} \left| \sum_{\substack{b\leq B \\ (p,b)=1}} \chi_2'(b) \right|^{2k} \right)^{\frac{1}{2k}}, \tag{5.20}$$

since in this case

$$\sum_{b\leq B} \chi'(b) = \sum_{b\leq B} \chi_1'\chi_2'(b) = \sum_{\substack{b\leq B \\ (p,b)=1}} \chi_2'(b).$$

We have that the first product in (5.20) becomes

$$\begin{aligned}\left(\sum_{\substack{p^-<q<p^+ \\ \chi_2'\neq\chi_0 \pmod q}}^{*} \left(\frac{H(D(p,q))^2}{pq}\right)^{\frac{2k}{2k-1}} \right)^{1-\frac{1}{2k}} &\ll \left(\sum_{p^-<q<p^+} \left(\frac{\log^2 p(\log\log p)^2}{p}\right)^{\frac{2k}{2k-1}} \right)^{1-\frac{1}{2k}} \\ &\ll \left(\frac{\sqrt{p}}{\log p} \left(\frac{\log^2 p(\log\log p)^2}{p}\right)^{\frac{2k}{2k-1}} \right)^{1-\frac{1}{2k}} \\ &\ll p^{-\frac{1}{2}-\frac{1}{4k}} (\log p)^{1+\frac{1}{2k}} (\log\log p)^2. \end{aligned} \tag{5.21}$$

As in the primitive case we extend the sum in the second product in (5.20) to a sum over all primitive characters modulo d for all modulus $d \leq Q = X$ since $q \ll X$. Using the

large sieve inequality, Theorem 2.2.22 we have that the second product in (5.20) becomes

$$\begin{aligned}\left(\sideset{}{^*}\sum_{\substack{p^-<q<p^+\\ \chi_2'\neq\chi_0 \pmod q}}\left|\sum_{\substack{b\leq B\\(p,b)=1}}\chi_2'(b)\right|^{2k}\right)^{\frac{1}{2k}} &\ll \left(\sideset{}{^*}\sum_{\substack{p^-<q<p^+\\ \chi_2'\neq\chi_0 \pmod q}}\left|\sum_{\substack{b\leq B^k\\(p,b)=1}}\tau_k(b;B)\chi_2'(b)\right|^{2}\right)^{\frac{1}{2k}}\\ &\ll \left(\sum_{\substack{d\leq X\\ \chi \pmod d\\ \chi \text{ primitive}}}\left|\sum_{\substack{b\leq B^k\\(p,b)=1}}\tau_k(b;B)\chi(b)\right|^{2}\right)^{\frac{1}{2k}}\\ &\ll \left(\sum_{\substack{d\leq X\\ \chi \pmod d\\ \chi \text{ primitive}}}\left|\sum_{\substack{b\leq B^k\\(p,b)=1}}\tau_k(b)\chi(b)\right|^{2}\right)^{\frac{1}{2k}}\\ &\ll \left((B^k+X^2)\sum_{b\leq B^k}|\tau_k(b)|^2\right)^{\frac{1}{2k}}\\ &\ll \left((B^k+X^2)B^k\log^{k^2-1}(B^k)\right)^{\frac{1}{2k}}. \end{aligned}\tag{5.22}$$

Combining (5.20), (5.21) and (5.22) gives

$$\begin{aligned}&A\sum_{\substack{p\leq X\\ p^-<q<p^+}}\frac{H(D(p,q))^2}{pq}\sum_{\substack{(\chi_1'\chi_2')^6=\chi_0 \pmod{pq}\\ \chi_1'\chi_2'\neq\chi_0 \pmod{pq}}}\left|\sum_{b\leq B}\chi_1'\chi_2'(b)\right|\\ \ll& A\left((B^k+X^2)B^k\log^{k^2-1}(B^k)\right)^{\frac{1}{2k}}\sum_{p\leq X}p^{-\frac{1}{2}-\frac{1}{4k}}(\log p)^{1+\frac{1}{2k}}(\log\log p)^2\\ \ll& AX^{\frac{1}{2}-\frac{1}{4k}}(\log X)^{\frac{1}{2k}}(\log\log X)^2\left((B^k+X^2)B^k\log^{k^2-1}(B^k)\right)^{\frac{1}{2k}}. \end{aligned}\tag{5.23}$$

Suppose that $B^k > X^2$ then we have that the RHS of (5.22) becomes

$$\left((B^k+X^2)B^k\log^{k^2-1}(B^k)\right)^{\frac{1}{2k}} \ll_k B\log^{\frac{k^2-1}{2k}}B, \tag{5.24}$$

for $k \geq 1$. Then suppose that $B^k \leq X^2$ for all $k \geq 1$. Then we can replace $\log B$ by $\log X$

in (5.22), which gives

$$\left((B^k+X^2)B^k\log^{k^2-1}(B^k)\right)^{\frac{1}{2k}} \ll_k \sqrt{B}X^{\frac{1}{k}}\log^{\frac{k^2-1}{2k}}(X). \tag{5.25}$$

Since

$$(B^k+X^2)^{\frac{1}{2k}} \ll_k \sqrt{B}+X^{\frac{1}{k}},$$

combining (5.24) and (5.25) with (5.23) gives

$$\begin{aligned}
&A\sum_{\substack{p\leq X\\ p^-<q<p^+}}\frac{H(D(p,q))^2}{pq}\sum_{\substack{(\chi_1'\chi_2')^6=\chi_0 \pmod{pq}\\ \chi_1'\chi_2'\neq\chi_0 \pmod{pq}}}\left|\sum_{b\leq B}\chi_1'\chi_2'(b)\right|\\
\ll_k &AX^{\frac{1}{2}-\frac{1}{4k}}(\log X)^{\frac{1}{2k}}(\log\log X)^2\left((B^k+X^2)B^k\log^{k^2-1}(B^k)\right)^{\frac{1}{2k}}\\
= &ABX^{\frac{1}{2}-\frac{1}{4k}}(\log X)^{\frac{1}{2k}}(\log\log X)^2\log^{\frac{k^2-1}{2k}}B+A\sqrt{B}X^{\frac{1}{2}+\frac{3}{4k}}(\log X)^{\frac{k}{2}}(\log\log X)^2. \quad (5.26)
\end{aligned}$$

Combining (5.19) and (5.26) gives that (5.11) becomes

$$\begin{aligned}
&A\sum_{\substack{p\leq X\\ p^-<q<p^+}}\frac{H(D(p,q))^2}{pq}\sum_{\substack{(\chi_1'\chi_2')^6=\chi_0 \pmod{pq}\\ \chi_1'\chi_2'\neq\chi_0 \pmod{pq}}}\left|\sum_{b\leq B}\chi_1'\chi_2'(b)\right|\\
\ll_k &ABX^{\frac{1}{2}-\frac{1}{4k}}(\log X)^{\frac{1}{2k}}(\log\log X)^2\log^{\frac{k^2-1}{2k}}B+A\sqrt{B}X^{\frac{1}{2}+\frac{5}{4k}}(\log X)^{\frac{k^2+1}{2k}}(\log\log X)^2.
\end{aligned}$$

Note that dividing the sum above by $4AB$ gives the length of the average with $A, B > X^\epsilon$ as in the average of the Lang-Trotter Conjecture for any $\epsilon > 0$. But we have considered only R_1, R_2 and R_3 and we still need to consider R_4 to obtain the length of the average for AB.

We now generalize these arguments for all L. Since $p_i = p + O_L(p)$ for $1 \leq i \leq L$ without loss of generality we can rearrange the primes $(p_1, \ldots, p_L)$ such that for $1 \leq i \leq s$ we have that $\chi_i' = \chi_0 \pmod{p_i}$ and for $s+1 \leq i \leq L$ we have that $\chi_i' \neq \chi_0 \pmod{p_i}$. It is possible that $s = 0$ in which case $\chi' := \chi_1' \cdots \chi_L'$ is primitive and by assumption we have that $s < L$. We have two cases to consider, either $s = 0$ in which case χ' is primitive, or

$0 < s < L$ in which case χ' is imprimitive.

We will consider the case when χ' is primitive first for the sum

$$A \sum_{\substack{p \leq X \\ p_i^- < p_{i+1} < p_i^+ \\ 1 \leq i \leq L-1}} \frac{1}{p_1 \cdots p_L} \prod_{j=1}^{L} H(D(p_j, p_{j+1})) \sum_{\substack{(\chi')^6 = \chi_0 \pmod{p_1 \cdots p_L} \\ \chi' \neq \chi_0 \pmod{p_1 \cdots p_L}}} |\mathcal{B}(\chi')| \tag{5.27}$$

in (5.10). In this case, the sum

$$\sum_{\substack{p \leq X \\ p_i^- < p_{i+1} < p_i^+ \\ 1 \leq i \leq L-1}}^{*}$$

denotes the sum over $p_1, \ldots, p_L$ and over characters χ' where $\chi' \neq \chi_0 \pmod{p_1 \cdots p_L}$. Since there are a bounded number of characters depending on L satisfying $(\chi')^6 = \chi_0 \pmod{p_1 \cdots p_L}$ from Hölder's inequality we have that (5.27) becomes

$$A \sum_{\substack{p \leq X \\ p_i^- < p_{i+1} < p_i^+ \\ 1 \leq i \leq L-1}} \prod_{j=1}^{L} \frac{H(D(p_j, p_{j+1}))}{p_j} \sum_{\substack{(\chi')^6 = \chi_0 \pmod{p_1 \cdots p_L} \\ \chi' \neq \chi_0 \pmod{p_1 \cdots p_L}}} \left| \sum_{b \leq B} \chi_1' \chi_2'(b) \right|$$

$$\ll_L A \left(\sum_{\substack{p \leq X \\ p_i^- < p_{i+1} < p_i^+ \\ 1 \leq i \leq L-1}}^{*} \prod_{j=1}^{L} \left(\frac{H(D(p_j, p_{j+1}))}{p_j} \right)^{\frac{2k}{2k-1}} \right)^{1-\frac{1}{2k}} \left(\sum_{\substack{p \leq X \\ p_i^- < p_{i+1} < p_i^+ \\ 1 \leq i \leq L-1}}^{*} \left| \sum_{b \leq B} \chi'(b) \right|^{2k} \right)^{\frac{1}{2k}}. \tag{5.28}$$

We have that the first product in (5.28) becomes

$$\begin{aligned}
&\left(\sum_{\substack{p\leq X\\ p_i^-<p_{i+1}<p_i^+\\ 1\leq i\leq L-1}}^{*}\prod_{j=1}^{L}\left(\frac{H(D(p_j,p_{j+1}))}{p_j}\right)^{\frac{2k}{2k-1}}\right)^{1-\frac{1}{2k}}\\
&\ll_L\left(\sum_{\substack{p\leq X\\ p_i^-<p_{i+1}<p_i^+\\ 1\leq i\leq L-1}}\left(\frac{\log^L p(\log\log p)^L}{p^{\frac{L}{2}}}\right)^{\frac{2k}{2k-1}}\right)^{1-\frac{1}{2k}}\\
&\ll_L\left(\sum_{p\leq X}\frac{p^{\frac{L-1}{2}}}{(\log p)^{L-1}}\left(\frac{\log^L p(\log\log p)^L}{p^{\frac{L}{2}}}\right)^{\frac{2k}{2k-1}}\right)^{1-\frac{1}{2k}}\\
&\ll_L X^{\frac{1}{2}-\frac{L+1}{4k}}(\log X)^{\frac{L}{2k}}(\log\log X)^L. \qquad (5.29)
\end{aligned}$$

We extend the sum in the second product in (5.28) to a sum over all primitive characters modulo d for all modulus $d\leq Q=X^L$, since $p_1\cdots p_L\ll_L X^L$. Using the large sieve

inequality, Theorem 2.2.22, gives

$$\begin{aligned}\left(\sum_{\substack{p\le X\\ p_i^-<p_{i+1}<p_i^+\\ 1\le i\le L-1}}^{*}\left|\sum_{b\le B}\chi'(b)\right|^{2k}\right)^{\frac{1}{2k}} &\ll_L \left(\sum_{\substack{p\le X\\ p_i^-<p_{i+1}<p_i^+\\ 1\le i\le L-1}}^{*}\left|\sum_{b\le B^k}\tau_k(b;B)\chi'(b)\right|^{2}\right)^{\frac{1}{2k}}\\ &\ll_L \left(\sum_{\substack{d\le X^L\\ \chi \pmod d\\ \chi \text{ primitive}}}\left|\sum_{b\le B^k}\tau_k(b;B)\chi(b)\right|^{2}\right)^{\frac{1}{2k}}\\ &\ll_L \left(\sum_{\substack{d\le X^L\\ \chi \pmod d\\ \chi \text{ primitive}}}\left|\sum_{b\le B^k}\tau_k(b)\chi(b)\right|^{2}\right)^{\frac{1}{2k}}\\ &\ll_L \left((B^k+X^{2L})\sum_{b\le B^k}|\tau_k(b)|^2\right)^{\frac{1}{2k}}\\ &\ll_L \left((B^k+X^{2L})B^k\log^{k^2-1}(B^k)\right)^{\frac{1}{2k}}. \end{aligned} \tag{5.30}$$

where we used Theorem 2.2.6 to bound the sum over b.

Combining (5.28), (5.29) and (5.30) gives

$$\begin{aligned}&A\sum_{\substack{p\le X\\ p_i^-<p_{i+1}<p_i^+\\ 1\le i\le L-1}}\frac{1}{p_1\cdots p_L}\prod_{j=1}^{L}H(D(p_j,p_{j+1}))\sum_{\substack{(\chi')^6=\chi_0 \pmod{p_1\cdots p_L}\\ \chi'\neq\chi_0 \pmod{p_1\cdots p_L}}}|\mathcal{B}(\chi')|\\ &\ll_L A\left((B^k+X^{2L})B^k\log^{k^2-1}(B^k)\right)^{\frac{1}{2k}}X^{\frac{1}{2}-\frac{L+1}{4k}}(\log X)^{\frac{L}{2k}}(\log\log X)^L. \end{aligned} \tag{5.31}$$

Suppose that $B^k > X^{2L}$ then we have that the RHS of (5.30) becomes

$$\left((B^k+X^{2L})B^k\log^{k^2-1}(B^k)\right)^{\frac{1}{2k}} \ll_{k,L} B\log^{\frac{k^2-1}{2k}}B, \tag{5.32}$$

for $k \ge 1$. Then suppose that $B^k \le X^{2L}$ for all $k \ge 1$. Then we can replace $\log B$ by

$\log X$ in (5.30), which gives

$$\left((B^k + X^{2L})B^k \log^{k^2-1}(B^k)\right)^{\frac{1}{2k}} \ll_{k,L} \sqrt{B} X^{\frac{L}{k}} \log^{\frac{k^2-1}{2k}}(X). \tag{5.33}$$

Since

$$(B^k + X^{2L})^{\frac{1}{2k}} \ll_{k,L} \sqrt{B} + X^{\frac{L}{k}},$$

combining (5.32) and (5.33) with (5.31) gives

$$\begin{aligned} A \sum_{\substack{p \leq X \\ p_i^- < p_{i+1} < p_i^+ \\ 1 \leq i \leq L-1}} \frac{1}{p_1 \cdots p_L} \prod_{j=1}^{L} H(D(p_j, p_{j+1})) \sum_{\substack{(\chi')^6 = \chi_0 \pmod{p_1 \cdots p_L} \\ \chi' \neq \chi_0 \pmod{p_1 \cdots p_L}}} |\mathcal{B}(\chi')| \\ = AB X^{\frac{1}{2} - \frac{L+1}{4k}} (\log X)^{\frac{L}{2k}} (\log\log X)^L \log^{\frac{k^2-1}{2k}} B + A\sqrt{B} X^{\frac{1}{2} + \frac{3L-1}{4k}} (\log X)^{\frac{k^2+L-1}{2k}} (\log\log X)^L. \end{aligned} \tag{5.34}$$

We now consider the imprimitive case. Fix $p_1, \ldots, p_s$ such that for $1 \leq i \leq s$ we have that $\chi_i' = \chi_0 \pmod{p_i}$ and for $s+1 \leq i \leq L$ we have that $\chi_i' \neq \chi_0 \pmod{p_i}$. The sum

$$\sum_{\substack{p \leq X \\ p_i^- < p_{i+1} < p_i^+ \\ 1 \leq i \leq s-1}}^{*}$$

denotes the sum over $p_1, \ldots, p_s$ where $\chi_i' = \chi_0 \pmod{p_i}$ for $1 \leq i \leq s$ and the sum

$$\sum_{\substack{p_i^- < p_{i+1} < p_i^+ \\ s+1 \leq i \leq L}}^{*}$$

denotes the sum over $p_{s+1}, \ldots, p_L$ where $\chi_i' \neq \chi_0 \pmod{p_i}$ for $s+1 \leq i \leq L$. As in the

primitive case, from Hölder's inequality we have that (5.27) becomes

$$A \sum_{\substack{p\leq X \\ p_i^-<p_{i+1}<p_i^+ \\ 1\leq i\leq L-1}} \prod_{j=1}^{L} \frac{H(D(p_j,p_{j+1}))}{p_j} \sum_{\substack{(\chi')^6=\chi_0 \pmod{p_1\cdots p_L} \\ \chi'\neq\chi_0 \pmod{p_1\cdots p_L}}} \left|\sum_{b\leq B} \chi_1'\chi_2'(b)\right|$$

$$\ll_L A \sum_{\substack{p\leq X \\ p_i^-<p_{i+1}<p_i^+ \\ 1\leq i\leq s-1}}^{*} \left(\sum_{\substack{p_i^-<p_{i+1}<p_i^+ \\ s+1\leq i\leq L}}^{*} \prod_{j=1}^{L} \left(\frac{H(D(p_j,p_{j+1}))}{p_j}\right)^{\frac{2k}{2k-1}} \right)^{1-\frac{1}{2k}}$$

$$\times \left(\sum_{\substack{p_i^-<p_{i+1}<p_i^+ \\ s+1\leq i\leq L}}^{*} \left| \sum_{\substack{b\leq B \\ (p_1\cdots p_s,b)=1}} \chi_{s+1}'\cdots\chi_L'(b) \right|^{2k} \right)^{\frac{1}{2k}}. \tag{5.35}$$

We have that the first product in (5.35) becomes

$$\left(\sum_{\substack{p_i^-<p_{i+1}<p_i^+ \\ s+1\leq i\leq L}}^{*} \prod_{j=1}^{L} \left(\frac{H(D(p_j,p_{j+1}))}{p_j}\right)^{\frac{2k}{2k-1}} \right)^{1-\frac{1}{2k}}$$

$$\ll_L \left(\sum_{\substack{p_i^-<p_{i+1}<p_i^+ \\ s+1\leq i\leq L}}^{*} \left(\frac{\log^L p(\log\log p)^L}{p^{\frac{L}{2}}}\right)^{\frac{2k}{2k-1}} \right)^{1-\frac{1}{2k}}$$

$$\ll_L \left(\frac{p^{\frac{L-s}{2}}}{(\log p)^{L-s}} \left(\frac{\log^L p(\log\log p)^L}{p^{\frac{L}{2}}}\right)^{\frac{2k}{2k-1}} \right)^{1-\frac{1}{2k}}$$

$$\ll_L p^{-\frac{s}{2}-\frac{L-s}{4k}} (\log p)^{s+\frac{L-s}{2k}} (\log\log p)^L. \tag{5.36}$$

As in the primitive case we extend the sum in the second product in (5.35) to a sum over all primitive characters modulo d for all modulus $d \leq Q = X^{L-s}$ since $p_{s+1}\cdots p_L \ll_L X^{L-s}$. Using the large sieve inequality, Theorem 2.2.22 and following as in the primitive

case we have that the second product in (5.35) becomes

$$\left(\sum_{\substack{p_i^-<p_{i+1}<p_i^+\\ s+1\le i\le L}}^{*}\left|\sum_{\substack{b\le B\\ (p_1\cdots p_s,b)=1}}\chi'_{s+1}\cdots\chi'_L(b)\right|^{2k}\right)^{\frac{1}{2k}}$$

$$\ll_L\left(\sum_{\substack{p_i^-<p_{i+1}<p_i^+\\ s+1\le i\le L}}^{*}\left|\sum_{\substack{b\le B^k\\ (p_1\cdots p_s,b)=1}}\tau_k(b;B)\chi'_{s+1}\cdots\chi'_L(b)\right|^{2}\right)^{\frac{1}{2k}}$$

$$\ll_L\left(\sum_{\substack{d\le X^{L-s}\\ \chi \pmod d\\ \chi \text{ primitive}}}\left|\sum_{\substack{b\le B^k\\ (p_1\cdots p_s,b)=1}}\tau_k(b;B)\chi(b)\right|^{2}\right)^{\frac{1}{2k}}$$

$$\ll_L\left(\sum_{\substack{d\le X^{L-s}\\ \chi \pmod d\\ \chi \text{ primitive}}}\left|\sum_{\substack{b\le B^k\\ (p_1\cdots p_s,b)=1}}\tau_k(b)\chi(b)\right|^{2}\right)^{\frac{1}{2k}}$$

$$\ll_L\left((B^k+X^{2(L-s)})\sum_{b\le B^k}|\tau_k(b)|^2\right)^{\frac{1}{2k}}$$

$$\ll_L\left((B^k+X^{2(L-s)})B^k\log^{k^2-1}(B^k)\right)^{\frac{1}{2k}}. \tag{5.37}$$

Combining (5.35), (5.36) and (5.37) gives

$$A\sum_{\substack{p\le X\\ p_i^-<p_{i+1}<p_i^+\\ 1\le i\le L-1}}\frac{1}{p_1\cdots p_L}\prod_{j=1}^{L}H(D(p_j,p_{j+1}))\sum_{\substack{(\chi')^6=\chi_0 \pmod{p_1\cdots p_L}\\ \chi'\neq\chi_0 \pmod{p_1\cdots p_L}}}|\mathcal{B}(\chi')|$$

$$\ll_L A\left((B^k+X^{2(L-s)})B^k\log^{k^2-1}(B^k)\right)^{\frac{1}{2k}}\sum_{\substack{p\le X\\ p_i^-<p_{i+1}<p_i^+\\ 1\le i\le s-1}}^{*}p^{-\frac{s}{2}-\frac{L-s}{4k}}(\log p)^{s+\frac{L-s}{2k}}(\log\log p)^L$$

$$\ll_L AX^{\frac{1}{2}-\frac{L-s}{4k}}(\log X)^{\frac{L-s}{2k}}(\log\log X)^L\left((B^k+X^{2(L-s)})B^k\log^{k^2-1}(B^k)\right)^{\frac{1}{2k}}. \tag{5.38}$$

Suppose that $B^k > X^{2(L-s)}$ then we have that the RHS of (5.37) becomes

$$\left((B^k + X^{2(L-s)})B^k \log^{k^2-1}(B^k)\right)^{\frac{1}{2k}} \ll_{k,L} B \log^{\frac{k^2-1}{2k}} B, \tag{5.39}$$

for $k \geq 1$. Then suppose that $B^k \leq X^{2(L-s)}$ for all $k \geq 1$. Then we can replace $\log B$ by $\log X$ in (5.37), which gives

$$\left((B^k + X^{2(L-s)})B^k \log^{k^2-1}(B^k)\right)^{\frac{1}{2k}} \ll_{k,L} \sqrt{B} X^{\frac{(L-s)}{2k}} \log^{\frac{k^2-1}{2k}}(X). \tag{5.40}$$

Since

$$(B^k + X^{2(L-s)})^{\frac{1}{2k}} \ll_{k,L} \sqrt{B} + X^{\frac{(L-s)}{k}},$$

combining (5.39) and (5.40) with (5.38) gives

$$\begin{aligned} &AX^{\frac{1}{2}-\frac{L-s}{4k}}(\log X)^{\frac{L-s}{2k}}(\log\log X)^L \left((B^k + X^{2(L-s)})B^k \log^{k^2-1}(B^k)\right)^{\frac{1}{2k}} \\ \ll_{L,k} &ABX^{\frac{1}{2}-\frac{1}{4k}}(\log X)^{\frac{L-1}{2k}}(\log\log X)^L \log^{\frac{k^2-1}{2k}} B \\ &+A\sqrt{B}X^{\frac{1}{2}+\frac{3(L-1)}{k}}(\log X)^{\frac{k^2+L-2}{2k}}(X)(\log\log X)^L, \end{aligned} \tag{5.41}$$

since $1 \leq L - s \leq L - 1$. Then combining (5.34) and (5.41) gives that (5.27) becomes

$$
\begin{aligned}
&A \sum_{\substack{p\le X\\ p_i^-<p_{i+1}<p_i^+\\ 1\le i\le L-1}} \frac{1}{p_1\cdots p_L}\prod_{j=1}^{L} H(D(p_j,p_{j+1})) \sum_{\substack{(\chi')^6=\chi_0 \pmod{p_1\cdots p_L}\\ \chi'\neq\chi_0 \pmod{p_1\cdots p_L}}} |\mathcal{B}(\chi')| \\
&\ll_{L,k} ABX^{\frac12-\frac{L+1}{4k}}(\log X)^{\frac{L}{2k}}(\log\log X)^L \log^{\frac{k^2-1}{2k}} B \\
&\quad + A\sqrt{B}X^{\frac12+\frac{3L-1}{4k}}(\log X)^{\frac{k^2+L-1}{2k}}(\log\log X)^L \\
&\quad + ABX^{\frac12-\frac{1}{4k}}(\log X)^{\frac{L-1}{2k}}(\log\log X)^L \log^{\frac{k^2-1}{2k}} B \\
&\quad + A\sqrt{B}X^{\frac12+\frac{3(L-1)}{k}}(\log X)^{\frac{k^2+L-2}{2k}}(X)(\log\log X)^L \\
&\ll_{L,k} ABX^{\frac12-\frac{1}{4k}}(\log X)^{\frac{L-1}{2k}}(\log\log X)^L \log^{\frac{k^2-1}{2k}} B \\
&\quad + A\sqrt{B}X^{\frac12+\frac{3L-1}{4k}}(\log X)^{\frac{k^2+L-1}{2k}}(\log\log X)^L. \qquad (5.42)
\end{aligned}
$$

Similarly, we deduce

$$
\begin{aligned}
&B \sum_{\substack{p\le X\\ p_i^-<p_{i+1}<p_i^+\\ 1\le i\le L-1}} \frac{1}{p_1\cdots p_L}\prod_{j=1}^{L} H(D(p_j,p_{j+1})) \sum_{\substack{(\chi)^4=\chi_0 \pmod{p_1\cdots p_L}\\ \chi\neq\chi_0 \pmod{p_1\cdots p_L}}} |\mathcal{A}(\chi)| \\
&\ll_{L,k} ABX^{\frac12-\frac{1}{4k}}(\log X)^{\frac{L-1}{2k}}(\log\log X)^L \log^{\frac{k^2-1}{2k}} A \\
&\quad + B\sqrt{A}X^{\frac12+\frac{3L-1}{4k}}(\log X)^{\frac{k^2+L-1}{2k}}(\log\log X)^L. \qquad (5.43)
\end{aligned}
$$

Thus, from (5.42) and (5.43) we have that (5.10) becomes

$$
\begin{aligned}
&\sum_{\substack{p\le X\\ p_i^-<p_{i+1}<p_i^+\\ 1\le i\le L-1}} \frac{1}{p_1\cdots p_L} \sum_{S,T\in\mathbb{F}(P)^*} w(P,S,T)\sum_{2\le j\le 3} S_j(P,S,T) \\
&\ll_{k,L} ABX^{\frac12-\frac{1}{4k}}(\log X)^{\frac{L-1}{2k}}(\log\log X)^L \log^{\frac{k^2-1}{2k}} AB \\
&\quad + (A\sqrt{B}+B\sqrt{A})X^{\frac12+\frac{3L-1}{4k}}(\log X)^{\frac{k^2+L-1}{2k}}(\log\log X)^L. \qquad (5.44)
\end{aligned}
$$

We now consider the final case $R_4(P,S,T)$ and define

$$W(P,\chi_i,\chi_i') = \sum_{\substack{1\le s_i,t_i<p_i\\ 1\le i\le L}} w(P,S,T)\chi_i(s_i)\chi_i'(t_i).$$

Then we have that

$$\begin{aligned}
&\sum_{\substack{p\le X\\ p_i^-<p_{i+1}<p_i^+\\ 1\le i\le L-1}} \frac{1}{p_1\cdots p_L} \sum_{S,T\in\mathbb{F}(P)^*} w(P,S,T)R_4(P,S,T)\\
=&\frac{1}{2^L}\sum_{\substack{p\le X\\ p_i^-<p_{i+1}<p_i^+\\ 1\le i\le L-1}} \prod_{j=1}^{L}\frac{1}{p_j(p_j-1)} \sum_{\substack{\chi^4(\chi')^6=\chi_0 \pmod{p_1\cdots p_L}\\ \chi\neq\chi_0,\chi'\neq\chi_0 \pmod{p_1\cdots p_L}}} W(P,\chi_i,\chi_i')\mathcal{A}(\overline{\chi})\mathcal{B}(\overline{\chi'}). \qquad (5.45)
\end{aligned}$$

We use Hölder's inequality to obtain

$$\begin{aligned}
&\left|\sum_{\substack{\chi^4(\chi')^6=\chi_0 \pmod{p_1\cdots p_L}\\ \chi\neq\chi_0,\chi'\neq\chi_0 \pmod{p_1\cdots p_L}}} W(P,\chi_i,\chi_i')\mathcal{A}(\overline{\chi})\mathcal{B}(\overline{\chi'})\right|\\
\le&\left|\sum_{\substack{\chi^4(\chi')^6=\chi_0 \pmod{p_1\cdots p_L}\\ \chi\neq\chi_0,\chi'\neq\chi_0 \pmod{p_1\cdots p_L}}} |W(P,\chi_i,\chi_i')|^2\right|^{\frac12}\\
&\times\left(\sum_{\substack{\chi^4(\chi')^6=\chi_0 \pmod{p_1\cdots p_L}\\ \chi\neq\chi_0,\chi'\neq\chi_0 \pmod{p_1\cdots p_L}}} |\mathcal{A}(\overline{\chi})|^4\right)^{\frac14}\left(\sum_{\substack{\chi^4(\chi')^6=\chi_0 \pmod{p_1\cdots p_L}\\ \chi\neq\chi_0,\chi'\neq\chi_0 \pmod{p_1\cdots p_L}}} \left|\mathcal{B}(\overline{\chi'})\right|^4\right)^{\frac14}. \qquad (5.46)
\end{aligned}$$

Thus, from the fourth power moment of Dirichlet characters, Theorem 2.2.29, we have that

$$\begin{aligned}
&\left(\sum_{\substack{\chi^4(\chi')^6=\chi_0 \pmod{p_1\cdots p_L}\\ \chi\neq\chi_0,\chi'\neq\chi_0 \pmod{p_1\cdots p_L}}} |\mathcal{A}(\overline{\chi})|^4\right)^{\frac14}\left(\sum_{\substack{\chi^4(\chi')^6=\chi_0 \pmod{p_1\cdots p_L}\\ \chi\neq\chi_0,\chi'\neq\chi_0 \pmod{p_1\cdots p_L}}} \left|\mathcal{B}(\overline{\chi'})\right|^4\right)^{\frac14}\\
\ll_L&\sqrt{AB}(p_1\cdots p_L)^{\frac12}\log^3(p_1\cdots p_L) \ll_L \sqrt{AB}(p_1\cdots p_L)^{\frac12}(\log^3 p). \qquad (5.47)
\end{aligned}$$

Now define

$$S' := (s'_1, \dots, s'_L) \quad \text{and} \quad T' := (t'_1, \dots, t'_L).$$

For a fixed character $\chi_1 \cdots \chi_L$ there are at most 6^L characters $\chi'_1 \cdots \chi'_L$ (or for any fixed character $\chi'_1 \cdots \chi'_L$ there are at most 4^L characters $\chi_1 \cdots \chi_L$) satisfying the condition

$$(\chi_1 \cdots \chi_L)^4 (\chi'_1 \cdots \chi'_L)^6 = \chi_0 \pmod{p_1 \cdots p_L}.$$

Then for the first character sum in (5.46), we extend the sum over all possible products of characters modulo $p_1 \cdots p_L$ (including the trivial character) and we obtain

$$\begin{aligned}
&\sum_{\substack{\chi^4(\chi')^6=\chi_0 \pmod{p_1\cdots p_L}\\ \chi\neq\chi_0,\chi'\neq\chi_0 \pmod{p_1\cdots p_L}}} |W(P,\chi_i,\chi'_i)|^2 \leq \sum_{\substack{\chi_i\\ 1\leq i\leq L}} \sum_{\substack{\chi'_i\\ 1\leq i\leq L}} |W(P,\chi_i,\chi'_i)|^2 \\
&\leq \sum_{S,T\in\mathbb{F}(P)^*} \sum_{S',T'\in\mathbb{F}(P)^*} w(P,S,T)\overline{w(P,S',T')} \sum_{\chi_i} \chi_i(s_i)\overline{\chi_i}(s'_i) \sum_{\chi'_i} \chi'_i(t_i)\overline{\chi'_i}(t'_i) \\
&= \prod_{i=1}^{L}(p_i-1)^2 \sum_{S,T\in\mathbb{F}(P)^*} |w(P,S,T)|^2 \\
&= p^{3L} \prod_{i=1}^{L} H(D(p_i,p_{i+1})) + O_L\left(p^{\frac{7L-1}{2}} \log^L p (\log\log p)^L\right) \qquad (5.48)
\end{aligned}$$

by (5.7) since $|w(P,S,T)|^2 = w(P,S,T)$. By combining (5.46), (5.47) and (5.48) we have that

$$\left| \sum_{\substack{\chi^4(\chi')^6=\chi_0 \pmod{p_1\cdots p_L}\\ \chi\neq\chi_0,\chi'\neq\chi_0 \pmod{p_1\cdots p_L}}} W(P,\chi_i,\chi'_i)\mathcal{A}(\overline{\chi})\mathcal{B}(\overline{\chi'}) \right| \ll_L \sqrt{AB}p^{2L}(\log^3 p) \prod_{i=1}^{L} H^2(D(p_i,p_{i+1})), \qquad (5.49)$$

and then plugging (5.49) into (5.45) gives

$$\sum_{\substack{p\leq X\\ p_i^-<p_{i+1}<p_i^+\\ 1\leq i\leq L-1}}\frac{1}{p_1\cdots p_L}\sum_{S,T\in\mathbb{F}(P)^*}w(P,S,T)R_4(P,S,T)$$
$$\ll_L\sqrt{AB}\sum_{p\leq X}\log^3 p\sum_{\substack{p_i^-<p_{i+1}<p_i^+\\ 1\leq i\leq L-1}}\prod_{j=1}^{L}\sqrt{H(D(p_j,p_{j+1}))}. \tag{5.50}$$

To obtain a better error term, instead of using the bound from (3.7) for $H(D(p_j,p_{j+1}))$, we use Cauchy-Schwarz, Proposition 3.2.3 and Proposition 3.2.4 to bound the inner sum in (5.50) to obtain

$$\sum_{\substack{p_i^-<p_{i+1}<p_i^+\\ 1\leq i\leq L-1}}\prod_{j=1}^{L}\sqrt{H(D(p_j,p_{j+1}))}$$
$$\leq\prod_{i=1}^{L-2}\left(\sum_{p_i^-<p_{i+1}<p_i^+}H(D(p_i,p_{i+1}))\sum_{p_i^-<p_{i+1}<p_i^+}1\right)^{\frac{1}{2}}$$
$$\times\left(\sum_{p_{L-1}^-<p_L<p_{L-1}^+}H(D(p_{L-1},p_L))H(D(p_L,p))\sum_{p_{L-1}^-<p_L<p_{L-1}^+}1\right)^{\frac{1}{2}}$$
$$\ll_L\prod_{i=1}^{L-2}\left(\frac{p_i}{\log p_i}\cdot\frac{\sqrt{p_i}}{\log p_i}\right)^{\frac{1}{2}}\left(\frac{p^{\frac{3}{2}}}{\log p}\cdot\frac{\sqrt{p}}{\log p}\right)^{\frac{1}{2}}$$
$$\ll_L\left(\frac{p^{\frac{3}{2}}}{\log^2 p}\right)^{\frac{L-2}{2}}\frac{p}{\log p}=\frac{p^{\frac{3L-2}{4}}}{\log^{L-1}p}. \tag{5.51}$$

From (5.50) and (5.51) we have that

$$\sum_{\substack{p\leq X\\ p_i^-<p_{i+1}<p_i^+\\ 1\leq i\leq L-1}}\frac{1}{p_1\cdots p_L}\sum_{S,T\in\mathbb{F}(P)^*}w(P,S,T)R_4(P,S,T)$$
$$\ll_L\sqrt{AB}\sum_{p\leq X}\frac{p^{\frac{3L-2}{4}}}{\log^{L-4}p}\ll_L\sqrt{AB}X^{\frac{3L+2}{4}}(\log X)^{3-L}. \tag{5.52}$$

Combining (5.44) and (5.52) gives the result. □

Chapter 6

Future work

6.1 Short and long term goals

The immediate goal after the completion of this thesis is to find an asymptotic result for the average number of amicable pairs to obtain a formula for the constant on average, which will then be compared with the constant conjectured by Jones in the amicable pairs case.

We conclude this thesis by discussing a few long range goals in the theory of amicable pairs and aliquot cycles for elliptic curves as well as other questions about the number of points on an elliptic curve defined over $\mathbb{Q}$, reduced by various primes with certain properties.

Nontrivial upper bounds not on average have been found for the Lang-Trotter conjecture and the Koblitz conjecture and a long term goal is to find a nontrivial upper bound for amicable pairs and aliquot cycles.

In the classical case of aliquot cycles, every integer n leads to a possibly non-repeating aliquot sequence

$$(n, s(n), (s \circ s)(n) := s_2(n), s_3(n), \ldots),$$

and is an aliquot cycle if $s_k(n) = n$ for some $k \geq 2$. A major open problem for aliquot

sequences is whether there exist starting values for which the sequence is unbounded. However, for elliptic curves, if we arrive at a prime p for which $\#E_p(\mathbb{F}_p)$ is not prime then the sequence can not be continued. In light of this feature, Silverman and Stange [SiSt2] also gave the following generalization of aliquot cycles.

Definition 6.1.1. Let $E/\mathbb{Q}$ be an elliptic curve and let

$$L(s, E) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$$

be the associated L-function of E. Consider the function

$$F_E : \mathbb{N} \to \mathbb{N}, F_E(n) = n + 1 - a_n.$$

A *type-L aliquot sequence* for $E/\mathbb{Q}$ is defined by considering an integer $n \in \mathbb{N}$ and repeatedly applying F_E. A *type-L aliquot cycle* is a type-L aliquot sequence that returns to its starting value.

Another interesting question in this subject is the study of *elliptic twins*, which are two distinct primes p, q such that $\#E_p(\mathbb{F}_p) = \#E_q(\mathbb{F}_q)$. Elliptic twins were first considered by Kowalski [Kow] where he explains why they are a natural analogue of classical twin primes and he gave a conjecture for the number of elliptic twins with $p \leq X$. A long term goal is to study the distribution of type-L aliquot cycles and elliptic twins and to see if an asymptotic can be given on average for these questions, and if so, to find a short length of the average as well.

Chapter 7

Bibliography

Bibliography

[BacSha] E. Bach and J. Shallit, Algorithmic number theory. Vol. 1. Efficient algorithms. Foundations of Computing Series. *The MIT Press*, Cambridge, MA, 1966.

[Ba1] S. Baier, The Lang-Trotter conjecture on average. *J. Ramanujan Math. Soc.* 22 (2007), 299–314.

[Ba2] S. Baier, A remark on the Lang-Trotter conjecture. *New directions in value-distribution theory of zeta and L-functions. Ber. Math.*, Shaker Verlag, Aachen (2009), 11–18.

[BCD] A. Balog, A. Cojocaru, and C. David. Average twin prime conjecture for elliptic curves. *Amer. J. Math.* 133 (2011), no. 5, 1179–1229.

[BanShp] W. Banks and I. Shparlinski, Sato-Tate, cyclicity, and divisibility statistics on average for elliptic curves of small height. *Israel J. Math.* 173 (2009), 253–277.

[CDKS] V. Chandee, C. David, D. Koukoulopoulos and E. Smith, Elliptic curves over finite fields with a given group structure. Preprint.

[Dav] H. Davenport, *Multiplicative Number Theory.* Third edition. Revised and with a preface by Hugh L. Montgomery. *Graduate Texts in Mathematics*, 74 Springer-Verlag, New York, 2000.

[DaPa] C. David and F. Pappalardi, Average Frobenius distributions of elliptic curves. *Internat. Math. Res. Notices* 1999, no. 4, 165–183.

[DaSm1] C. David and E. Smith, Elliptic curves with a given number of points over finite fields. *Compos. Math.* 149 (2013), no. 2, 175–203.

[Deu] M. Deuring, Die Typen der Multiplikatorenringe elliptischer Funktionenkörper. *Abh. Math. Sem. Univ. Hamburg*, 14 (1941), no. 1, 197–272.

[Elk] N. Elkies, The existence of infinitely many supersingular primes for every elliptic curve over $\mathbb{Q}$. *Invent. Math.* 89 (1987), no. 3, 561–567.

[FoMu] E. Fouvry and M. R. Murty, On the distribution of supersingular primes. *Canad. J. Math.* 48 (1996), no. 1, 81–104.

[FrIw1] J. Friedlander and H. Iwaniec, On Bombieri's asymptotic sieve. *Ann. Scuola Norm. Sup. Pisa Cl. Sci.* (4) 5 (1978), no. 4, 719–756.

[FrIw2] J. Friedlander and H. Iwaniec, The divisor problem for arithmetic progressions. *Acta Arith.* 45 (1985), 273–277.

[GrSo] A. Granville and K. Soundararajan, The distribution of values of $L(1, \chi_d)$. *Geom. Funct. Anal.*, 13 (2003), no. 5, 992–1028.

[HaWr] G. Hardy and E. Wright, *An introduction to the theory of numbers*. Sixth edition. Revised by D. R. Heath-Brown and J. H. Silverman. With a foreword by Andrew Wiles. Oxford University Press, Oxford, 2008.

[HSBT] M. Harris, N. Shepherd-Barron and R. Taylor, A family of Calabi-Yau varieties and potential automorphy. *Ann. of Math.* (2) 171 (2010), no. 2, 779–813.

[Jon1] N. Jones, Averages of elliptic curve constants. *Math. Ann.* 345 (2009), no. 3, 685–710.

[Jon2] N. Jones, Elliptic aliquot cycles of fixed length. Preprint.

[Kob] N. Koblitz, Primality of the number of points on an elliptic curve over a finite field. *Pacific J. Math.* 131 (1998), no. 1, 157–165.

[Kow] E. Kowalski, Analytic problems for elliptic curves. *J. Ramanujan Math. Soc.* 21 (2006), no. 1, 19–114.

[LPZ] A. Languasco, A. Perelli and A. Zaccagnini. On the Montgomery-Hooley Theorem in short intervals. *Mathematika*, 56 (2010), no. 2, 231–243.

[LaTr] S. Lang and H. Trotter, *Frobenius distributions in GL_2-extensions*. Lecture Notes in Mathemtics, Vol. 504. Springer-Verlag, Berlin-New York, 1976. Distribution of Frobenius automorphismsin GL_2-extensions of the rational numbers.

[Len] H. Lenstra, Factoring integers with elliptic curves. *Ann. of Math.* (2) 126 (1987), no. 3, 649–673.

[Maz] B. Mazur, Rational points of abelian varieties with values in towers of number fields. *Invent. Math.* 18 (1972), 183–266.

[Se1] J-P. Serre, *Abelian l-adic representations and elliptic curves*, Benjamin, New York-Amsterdam, 1968.

[Se2] J-P. Serre, Propriétés galoisiennes des points d'ordre fini des courbes elliptiques, *Invent. Math.* 15 (1972), 259–331.

[Sil1] J. Silverman, *The arithmetic of elliptic curves*, *Graduate Texts in Mathematics*, 106 Springer-Verlag, New York, 1986.

[Sil2] J. Silverman, *Advanced topics in the arithmetic of elliptic curves*, *Graduate Texts in Mathematics*, 151 Springer-Verlag, New York, 1994.

[SiSt1] J. Silverman and K. Stange, Terms in elliptic divisibility sequences divisible by their indices. *Acta Arith.* 146 (2011), no. 4, 355–378.

[SiSt2] J. Silverman and K. Stange, Amicable pairs and aliquot cycles for elliptic curves. *Exp. Math.* 20 (2011), no. 3, 329–357.

[Smy] C. Smyth, The terms in Lucas sequences divisible by their indices. *J. Integer Seq.* 13 (2010), no. 2, Article 10.2.4, 18 pp.

[Ste] S. Stepanov, *Arithmetic of Algebraic Curves*. Translated from the Russian by Irene Aleksanova. Monographs in Contemporary Mathematics. Consultants Bureau, New York, 1994.

[Te] G. Tenenbaum, *Introduction to analytic and pobabilistic number theory*. Translated from the second French edition (1995) by C. B. Thomas. Cambridge Studies in Advanced Mathematics, 46. Cambridge University Press, Cambridge, 1995.

[Zyw] D. Zywina, A refinement of Koblitz's conjecture. *Int. J. Number Theory* 7 (2011), no. 3, 739–769.